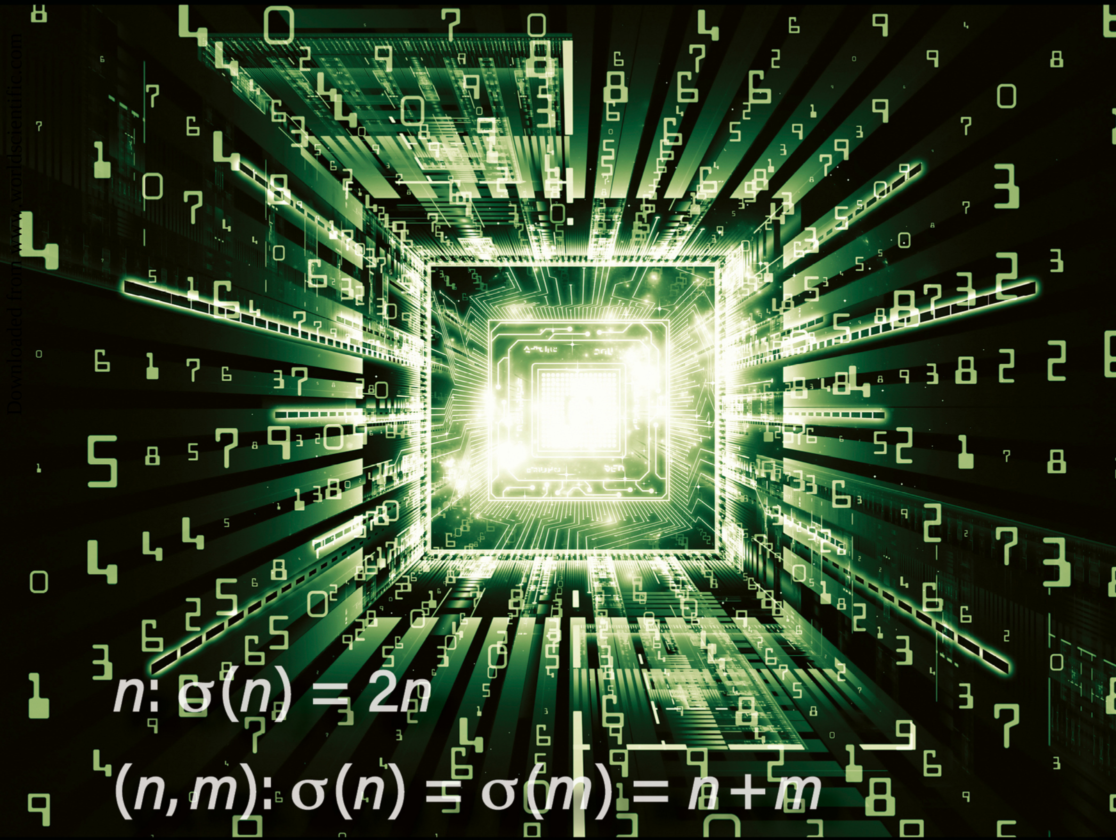
Selected Chapters of Number Theory: Special Numbers – Volume 2

Perfect and Amicable Numbers

Elena Deza


$n\colon \sigma(n) = 2n$
$(n, m)\colon \sigma(n) = \sigma(m) = n + m$

World Scientific

Perfect and Amicable Numbers

Selected Chapters of Number Theory: Special Numbers

Series Editor: Elena Deza (*Moscow State Pedagogical University, Russia*)

Published

Vol. 2 *Perfect and Amicable Numbers*
by Elena Deza

Vol. 1 *Mersenne Numbers and Fermat Numbers*
by Elena Deza

Selected Chapters of Number Theory: Special Numbers – Volume 2

Perfect and Amicable Numbers

Elena Deza

Moscow State Pedagogical University, Russia

World Scientific

NEW JERSEY • LONDON • SINGAPORE • BEIJING • SHANGHAI • HONG KONG • TAIPEI • CHENNAI • TOKYO

Published by

World Scientific Publishing Co. Pte. Ltd.
5 Toh Tuck Link, Singapore 596224
USA office: 27 Warren Street, Suite 401-402, Hackensack, NJ 07601
UK office: 57 Shelton Street, Covent Garden, London WC2H 9HE

Library of Congress Cataloging-in-Publication Data
Names: Deza, Elena, author.
Title: Perfect and amicable numbers / Elena Deza, Moscow State Pedagogical University, Russia.
Description: New Jersey : World Scientific, [2023] | Series: Selected chapters of number theory : special numbers ; volume 2 | Includes bibliographical references and index.
Identifiers: LCCN 2022026779 | ISBN 9789811259623 (hardcover) | ISBN 9789811259630 (ebook) | ISBN 9789811259647 (ebook other)
Subjects: LCSH: Perfect numbers. | Amicable numbers.
Classification: LCC QA242 .D49 2023 | DDC 512.7/4--dc23/eng20220829
LC record available at https://lccn.loc.gov/2022026779

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

Copyright © 2023 by World Scientific Publishing Co. Pte. Ltd.

All rights reserved. This book, or parts thereof, may not be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording or any information storage and retrieval system now known or to be invented, without written permission from the publisher.

For photocopying of material in this volume, please pay a copying fee through the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, USA. In this case permission to photocopy is not required from the publisher.

For any available supplementary material, please visit
https://www.worldscientific.com/worldscibooks/10.1142/12928#t=suppl

Desk Editors: Soundararajan Raghuraman/Adam Binnie/Shi Ying Koe

Typeset by Stallion Press
Email: enquiries@stallionpress.com

Printed in Singapore

Mathematics is the queen of the Sciences and Number Theory is the queen of Mathematics.
— Gauss

God invented the integers; all else is the work of man.
— Kronecker

I know numbers are beautiful. If they aren't beautiful, nothing is.
— Erdős

Dedicated to Senya

This page intentionally left blank

Preface

Special numbers, among integers, are an important part of number theory, general mathematics, and several applied areas (such as cryptography).

While the "names" of some of them (Fermat numbers, Mersenne numbers, Fibonacci numbers, Catalan numbers, Bernoulli numbers, Stirling numbers, etc.) are known to every mathematician, actual information on them is often scattered in the special literature. There are only few books which systematically present their history and properties while giving the main proofs.

Moreover, although such books exist (see, for example, [Bond93], [CoGu96], [Hogg69], [Line86], [LiNi96], [KLS01], [SlPl95], [Uspe76], [Voro61], and [Yan96]), many new results have appeared during the several decades after their publication; so, this material should be updated and reworked.

We should also mention several classical monographs on number theory ([Apos86], [Dick05], [HaWr79], [MSC96], [Ribe89], [Ribe96], [Sier64], etc.). Those are basic books of fundamental importance. But they treat number theory as a whole and special numbers get only a small place there.

Our first book on special numbers, the monograph *Figurate Numbers* [DeDe12], deals with all problems of polygonal numbers and their different generalizations, giving the full retrospective of the history of most known classes of special integers.

In the series selected chapters of Number Theory: Special Numbers, we are going to consider, following a similar structure, the history and properties of several other famous classes of special numbers.

The books offered in this series are: *Mersenne and Fermat Numbers*, *Perfect and Amicable Numbers*, *Stirling Numbers*, *Catalan Numbers*, *Bernoulli Numbers*, and *Euler Numbers*.

So, the main purpose of the series is to give a complete presentation of the theory of several classes of classical special numbers, considering much of their properties, facts, and theorems with full proofs.

In particular, we expect:

- to find and to organize much of scattered material;
- to present updated material with all details in a clear and unified way;
- to consider all ranges of well-known and hidden connections of a given set of numbers with different mathematical problems;
- to draw up a system of multilevel tasks.

The first book of the series, *Mersenne Numbers and Fermat Numbers*, was published in 2021.

Mersenne numbers, i.e., positive integers of the form $M_n = 2^n - 1,\ n \in \mathbb{N}$, were considered by Euclid (fourth century BC) and later by many Arabic and European mathematicians in an attempt to find all perfect numbers. Finally, the numbers of the form $2^n - 1$ were named after Marin Mersenne (1588–1648), a French monk and mathematician, who discussed them in his work *Cogita physico mathematics* (1644) and stated some conjectures about the number's occurrence.

A *Fermat number* F_n is a positive integer of the form $F_n = 2^{2^n} + 1$, $n \in \mathbb{Z},\ n \geq 0$.

Fermat numbers, i.e., positive integers of the form $F_n = 2^{2^n} + 1$, $n \in \mathbb{Z}$, $n \geq 0$, were studied by the 17th century French lawyer and mathematician Pierre de Fermat (1607–1665), who conjectured (1650) that these numbers would always give a prime for $n = 0, 1, 2, \ldots$. In fact, the first five Fermat numbers are primes: $F_0 = 3$,

$F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$. But in 1732, Leonhard Euler (1707–1783), a Swiss-Russian mathematician, physicist, astronomer, geographer, logician, and engineer, found that F_5 is a composite number. So, Fermat's conjecture that F_n is always prime is clearly false. Moreover, beyond F_4, no further Fermat primes have been found.

Nowadays, the theory of Mersenne and Fermat numbers contains many interesting mathematical facts and theorems as well as a lot of important applications. The mathematical part of this theory is closely connected with classical arithmetic and number theory. It contains much information about divisibility properties of Mersenne and Fermat numbers, their connections with other classes of special numbers, etc. Moreover, Mersenne and Fermat numbers are used in the construction of new large primes and have numerous applications in contemporary cryptography.

The second book of the series is devoted to perfect and amicable numbers as well as their numerous analogues and generalizations.

Perfect and amicable numbers, as well as a majority of classes of special numbers, have a long and rich history connected with the names of many famous mathematicians. This history is mainly an important part of the history of prime numbers since the main formulas, generating perfect and amicable pairs, depend on the proper choice of one or several primes of special form.

A *perfect number* is a positive integer n which is equal to the sum of its positive divisors: $n = \sum_{d|n, d<n} d$. The first four perfect numbers are 6, 28, 496, and 8128.

It is not known when perfect numbers were first studied. It is quite likely, although not certain, that the Egyptians would have come across such numbers. Perfect numbers were studied by Pythagoras and his followers, more for their mystical properties than for their number-theoretic properties. The first recorded mathematical result concerning perfect numbers which is known occurs in Euclid's *Elements* written around 300 BC. Euclid proved that all even perfect numbers have the form $2^{k-1}(2^k - 1)$, where $2^k - 1$ is a prime. Two millennia later, Euler proved the converse of Euclid's result by proving that every even perfect number had to be of this form.

So, the *Euclid–Euler theorem* states that *an even positive integer is a perfect number if and only if it can be represented as a product* $2^{k-1}(2^k - 1)$, *where* $2^k - 1$ *is a prime.* In fact, it is a Mersenne prime, so there exists a one-to-one relationship between even perfect numbers and Mersenne primes; each Mersenne prime generates one even perfect number, and vice versa.

As for odd perfect numbers, it is unknown whether any odd perfect numbers exist, though various results have been obtained.

Amicable numbers are two different natural numbers (m, n) related in such a way that the sum of the proper divisors of each is equal to the other number: $n = \sum_{d|m, d<m} d$, and $m = \sum_{d|n, d<n} d$. The smallest pair of amicable numbers $(220, 284)$ was known to the Pythagoreans, who credited them with many mystical properties. A general formula by which some of these numbers could be derived was invented circa 850 by the Iraqi mathematician Thābit ibn Qurra. The *Thābit's rule* states that *if* $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$, *and* $r = 9 \cdot 2^{2n-1} - 1$ *are primes, then* $A = 2^n pq$ *and* $B = 2^n r$ *are a pair of amicable numbers.* This formula gives the pairs $(220, 284)$ for $n = 2$, $(17296, 18416)$ for $n = 4$, and $(9363584, 9437056)$ for $n = 7$, but no other such pairs are known. The *Euler's rule* (1747–1750) generalizes the Thābit ibn Qurra theorem and creates additional amicable pairs for $(m, n) = (1, 8), (29, 40)$ with no others being known. However, Euler overall found 58 new pairs bringing the total number of pairs to 61.

At present, 51 perfect numbers are known, $2^{88}(2^{89} - 1)$ being the last to be discovered by hand calculations in 1911 (although not the largest found by hand calculations), all others being found using a computer. At the moment, the largest known Mersenne prime is $2^{82589933} - 1$ (which is also the largest known prime) and the corresponding largest known perfect number is $2^{82589932}(2^{82589933} - 1)$. It was discovered in 2018 and contains more than 23 million digits. As of 2021, there are over 10^9 known amicable pairs, the biggest one with two 24073-digit numbers.

Nowadays, the theory of perfect and amicable numbers contains many interesting mathematical facts and theorems as well as a lot of important computer algorithms for searching new large elements of these two famous classes of special numbers.

The mathematical part of this theory is closely connected with classical arithmetic and number theory. It contains much information about divisibility properties of perfect and amicable numbers, structure and properties of their generalizations and analogues (sociable numbers, multiperfect numbers, quasi-perfect and quasi-amicable numbers, etc.), their connections with other classes of special numbers, etc.

Moreover, perfect and amicable numbers are involved in the search of new large primes and have numerous connections with contemporary cryptography. For these applications, one should study the well-known deterministic and probabilistic primality tests, standard algorithms of integer factorization, the questions and open problems of computational complexity theory.

The book deals in detail with all these aspects.

In Chapter 1, we consider some important questions of elementary number theory, which will be used later. In elementary number theory, integers are studied without the use of techniques from other mathematical fields. Questions of divisibility, use of the Euclidean algorithm to compute greatest common divisors, factorization of integers into prime numbers, investigation of the behavior of prime numbers and congruences, and properties and applications of continued fractions belong to this part of elementary mathematics. Several important discoveries of this field are the Fermat's little theorem, the Euler's theorem, the Chinese remainder theorem, and the law of quadratic reciprocity.

In this chapter, we collect: the basic facts of the theory of divisibility of integers; main questions of modular arithmetic; algorithms of solutions of congruences; a base for the theory of quadratic residues (including properties of Legendre symbol and Jacobi symbol); definitions and properties of multiplicative order, primitive roots, and indexes (discrete logarithms) modulo n; some important elementary properties of continued fractions as well as their applications to rational approximations and to solutions of several important classes of Diophantine equations. We represent all needed definitions, give many examples, collect the main properties of considered mathematical objects without proofs but with a large list of possible references.

As the main part of the theory of perfect and amicable numbers focuses on the questions of the properties of their divisors, in Chapter 2, we give the basic theory of arithmetic functions, including the history of the question, a large list and elementary properties of well-known additive and multiplicative functions, the properties of such arithmetic functions as the floor function, the Möbius function, the Euler's totient function, the divisor functions, an exclusive collection of the famous and hidden connections of considered functions with different classes of special numbers.

Chapter 3 contains a rich review of the mathematical theory of perfect numbers with all needed proofs and many examples. Starting with the history of the question, we consider the role of divisor functions in the construction and the studies of perfect numbers, prove the Euclid–Euler theorem, list elementary properties of perfect numbers, including the questions of their divisibility. As the main part of the theory of even perfect numbers is connected with problems of primality of Mersenne numbers, we consider the well-known properties of prime divisors of Mersenne numbers as well as prove the algorithm of Lucas–Lehmer primality test for Mersenne numbers. Moreover, we give a large collection of possible connections of perfect numbers with other classes of special numbers, including Fermat numbers and elements of Pascal's triangle. Lastly, we present a rich list of open problems in number theory, connected with perfect numbers.

In Chapter 4, we consider similarly main questions of the theory of amicable numbers. The structure of Chapter 4 is the same as the structure of Chapter 3. Starting with the history of the question, we consider the role of divisor functions in the construction and study of amicable numbers, prove the Thābit's and the Euler's theorems, prove elementary properties of amicable numbers. Then, we give a large collection of the possible connections of amicable numbers with other classes of special numbers and present a rich list of open problems in number theory connected with amicable pairs.

Chapter 5 contains some important questions concerning the well-known generalizations and analogues of perfect and amicable numbers. After a small historical review of the problem, we give a detailed list of all well-known relatives of perfect numbers (multiply perfect, superperfect, quasi-perfect, almost perfect, and many other numbers) as well as those of amicable numbers. The theory of sociable numbers is given in connection with the properties of aliquot sequences. As before, we collect the most important open problems in this part of number theory.

In a small Chapter 6, we collect some remarkable individual numbers, related to the theory of perfect and amicable numbers as well as to the general theory of prime numbers.

In Chapter 7, a huge “Mini Dictionary” lists all classes of special numbers mentioned in the text.

Chapter 8 “Exercises” contains a big exclusive collection of problems connected with the theory of perfect and amicable numbers, with full solutions or, at least, with short hints of proofs.

The target audience of the book consists of university professors and students (especially graduate ones) interested in number theory, general algebra, cryptography, and related fields, as well as school teachers, general audience, and amateur mathematicians.

Specifically, Chapters 2, 3, and 4 are accessible to undergraduate students and general readers of mathematics, while Chapter 5 is slightly more difficult.

The book is so organized that it can be used as a source material for individual scientific work of university students and even, partially, of school students. In fact, the material of the book was already used for the preparation of bachelor’s and master’s theses of many students of Moscow State Pedagogical University.

This page intentionally left blank

About the Author

Elena (Ivanovna) Deza is a doctor of pedagogical sciences (2012) and a candidate of physical and mathematical sciences (1993). She is currently a full professor at Moscow State Pedagogical University and head of the Department of Number Theory at the Institute of Mathematics and Informatics of Moscow State Pedagogical University. She is an academician of the International Academy of Sciences of Pedagogical Education, Moscow, and the Concord Academy, France.

She graduated from the Faculty of Mathematics of the Moscow State Pedagogical Institute in 1983, after which she worked at the Moscow Forestry Academy from 1983 to 1988. From 1988 to the present, she has been working as an assistant (1988), an assistant professor (1993), and a full professor (2006) at Moscow State Pedagogical University.

Her areas of professional interest include analytic number theory, discrete mathematics, the theory of finite generalized metric spaces, the theory of special numbers, and higher education didactics.

Elena Ivanovna has authored more than 300 scientific papers on mathematics and didactics and more than 20 textbooks on number theory, cryptography, and discrete mathematics in Russian. She has also authored several monographs in English, devoted to distances and special numbers.

This page intentionally left blank

Notations

- X – a set; $X = \{x_1, \ldots, x_n\}$ — a *finite set*; $|X| = n$ — the number n of elements in the finite set $X = \{x_1, \ldots, x_n\}$.
- $\mathbb{N} = \{1, 2, 3, \ldots\}$ — the set of *positive integers* (or *natural numbers*).
- $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ — the set of *integers*.
- $\mathbb{Q}$ — the set of *rational numbers*.
- $\mathbb{R}$ — the set of *real numbers*.
- $\mathbb{C} = \{a + b \cdot i : a, b \in \mathbb{R}, i^2 = -1\}$ — the set of *complex numbers*.
- $b|a$ — a non-zero integer b divides an integer a: $a = bc$, where $c \in \mathbb{Z}$.
- $gcd(a_1, \ldots, a_n)$ — *greatest common divisor* of integers $a_1, \ldots, a_n$, at least one of which is not equal to 0, i.e., the greatest integer dividing $a_1, \ldots, a_n$. If $gcd(a_1, \ldots, a_n) = 1$, the numbers $a_1, \ldots, a_n$ are called *relatively prime* or *coprime*; if $gcd(a_i, a_j) = 1$ for any distinct $i, j \in \{1, \ldots, n\}$, the numbers $a_1, \ldots, a_n$ are called *pairwise relatively prime*.
- $lcm(a_1, \ldots, a_n)$ — *least common multiple* of non-zero integers $a_1, \ldots, a_n$, i.e., the least positive integer divided by $a_1, \ldots, a_n$.
- $rest(a, b)$ — the *remainder* of an integer a after its *integer division* by a positive integer b: $a = b \cdot q + rest(a, b)$, where $q, rest(a, b) \in \mathbb{Z}$ and $0 \leq rest(a, b) < b$.
- $P = \{2, 3, 5, 7, 11, 13, 17, 19, \ldots\}$ — the set of *prime numbers*, i.e., the positive integers having exactly two positive integer divisors; $p, q, p_1, p_2, \ldots, p_k, \ldots, q_1, q_2, \ldots, q_s, \ldots$ — prime numbers.

- $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, $p_1 < \cdots < p_k \in P$, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$ — the *prime factorization* of a positive integer $n > 1$, i.e., its representation as a product of positive integer powers of different prime numbers $p_1, \ldots, p_k$.
- $S = \{4, 6, 8, 9, 10, 12, 14, 15, 16, 18, \ldots\}$ — the set of *composite numbers*, i.e., the positive integers having more than two positive integer divisors.
- $n = (c_s c_{s-1} \ldots c_1 c_0)_g = c_s g^s + c_{s-1} g^{s-1} + \cdots + c_1 g + c_0$, $g \in \mathbb{N} \backslash \{1\}$, $0 \leq c_i \leq g - 1$, $c_s \neq 0$ — representation of a positive integer n in *base g*.
- $\lfloor x \rfloor$, $x \in \mathbb{R}$ — *floor function*: the largest integer less than or equal to x.
- $\{x\}$, $x \in \mathbb{R}$ — *fractional value* of x: $\{x\} = x - \lfloor x \rfloor$.
- $\lceil x \rceil$, $x \in \mathbb{R}$ — *ceiling function*: the smallest integer greater than or equal to x.
- $||x|| = \min\{\{x\}, 1 - \{x\}\}$, $x \in \mathbb{R}$ — the distance between x and the integer closest to x.
- $\phi(n)$, $n \in \mathbb{N}$ — *Euler's totient function*: the number of positive integers that are relatively prime to n: $\phi(n) = |\{x \in \mathbb{N} : x \leq n, gcd(x, n) = 1\}|$.
- $\lambda(n)$, $n \in \mathbb{N}$ — *Carmichael function*: for prime $p \geq 3$ and positive integer α, $\lambda(p^\alpha) = \phi(p^\alpha)$; for positive integer $\alpha \geq 3$, $\lambda(2^\alpha) = 2^{\alpha-2}$, while $\lambda(2) = 1$, and $\lambda(4) = 2$; moreover, $\lambda(p_1^{\alpha_1} \ldots p_k^{\alpha_k}) = lcm(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_k^{\alpha_k}))$.
- $\mu(n)$, $n \in \mathbb{N}$ — *Möbius function*: $\mu(1) = 1$, $\mu(n) = (-1)^k$, if $n = p_1 \cdot \ldots \cdot p_k$ is a product of k distinct primes, and $\mu(n) = 0$ if n has repeated prime factors.
- $\pi(x) = \sum_{p \leq x} 1$, $x \in \mathbb{R}, x \geq 0$ — *prime counting function*: the number of primes less than or equal to a given non-negative real number x.
- $\tau(n) = \sum_{d|n} 1$, $n \in \mathbb{N}$ — *tau function* (or *number of divisors function*): the number of positive integer divisors of a positive integer n.
- $\sigma(n) = \sum_{d|n} d$, $n \in \mathbb{N}$ — *sigma function* (or *sum of divisors function*): the sum of positive integer divisors of a positive integer n.

- $\sigma_k(n) = \sum_{d|n} d^k$, $n \in \mathbb{N}, k \in \mathbb{C}$ — *divisor function*: the sum of the kth powers of positive integer divisors of a positive integer n. In particular, $\sigma_0(n) = \tau(n)$ and $\sigma_1(n) = \sigma(n)$.
- $s(n) = \sum_{d|n,\ d\neq n} d$, $n \in \mathbb{N}$ — *aliquot sum function* (or *restricted divisor function*): the sum of all proper divisors of a positive integer n, i.e., all positive integer divisors of n other than n itself.
- $\nu(n)$ — the number of distinct prime divisors of a positive integer n.
- $\Lambda(n)$, $n \in \mathbb{N}$ — *Mangoldt function*: $\Lambda(n) = \log p$ if $n = p^k$, where $p \in P$ and $k \in \mathbb{N}$, and $\Lambda(n) = 0$ otherwise.
- $a \equiv b(mod\ n)$ — an integer a is *congruent* to an integer b modulo n, $n \in \mathbb{N}$, i.e., $n|(a-b)$.
- $[a]_n = \mathbf{a}_n = \{x \in \mathbb{Z} : x \equiv a(mod\ n)\} = \{\dots, a-2n, a-n, a, a+n, a+2n, a+3n, \dots\}$ — *residue class* (*of* a) *modulo* n: the set of all integers congruent to a modulo n. Any representative r_a of $[a]_n$ is called *residue* of a modulo n. The smallest non-negative representative of $[a]_n$ is called *smallest non-negative residue* of a modulo n; it is the *remainder* $rest(a, n)$ of a after its *integer division* by n. The smallest in absolute value representative of $[a]_n$ is called *minimal residue* of a modulo n.
- $(Z/nZ, +, \cdot)$, where $Z/nZ = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$ — the *factor ring* (or *quotient ring*) modulo n; for a prime number p, the ring $(Z/pZ, +, \cdot)$ is a (finite) field.
- $(Z/nZ^*, \cdot)$, where $Z/nZ^* = \{[1]_n, [2]_n, \dots, [n-1]_n\}$ — the *multiplicative group of the factor ring* $(Z/nZ, +, \cdot)$.
- $(\frac{a}{p})$ — *Legendre symbol*: $(\frac{a}{p}) = 1$, if an integer a, relatively prime to an odd prime number p, is a *quadratic residue modulo* p (i.e., the congruence $x^2 \equiv a(mod\ p)$ has a solution $x_0 \in \mathbb{Z}$), $(\frac{a}{p}) = -1$ if an integer a, relatively prime to an odd prime number p, is a *quadratic non-residue modulo* p (i.e., the congruence $x^2 \equiv a(mod\ p)$ does not have a solution), and $(\frac{a}{p}) = 0$ if $p|a$.
- $(\frac{a}{n}) = (\frac{a}{p_1})^{\alpha_1} \cdot \ldots \cdot (\frac{a}{p_k})^{\alpha_k}$ for odd positive integer $n = p_1^{\alpha_1} \cdot \ldots \cdot {}_k^{\alpha_k}$ — *Jacobi symbol*. When n is a prime, the Jacobi symbol $(\frac{a}{n})$ reduces to the Legendre symbol.

- $ord_n\, a$ — *multiplicative order* (or *modulo order*) of an integer a, relatively prime to n, modulo n: the smallest positive integer exponent γ for which $a^\gamma \equiv 1 (mod\ n)$.
- $ind_g\ a$ — *index* (or *discrete logarithm*) of an integer a with respect to the base g modulo n, i.e., the only integer $\beta \in [0, \phi(n) - 1]$ for which $a \equiv g^\beta (mod\ n)$. Here, $n \in \{2, 4, p^\alpha, 2p^\alpha\}$, where $p \in P\backslash\{2\}$, $\alpha \in \mathbb{N}$, g — *primitive root modulo* n (i.e., $ord_n\, g = \phi(n)$), and a — an integer, relatively prime to n.
- $[a_0, a_1, \ldots, a_n, \ldots] = a_0 + \frac{1}{a_1 + \frac{1}{\cdots \frac{1}{a_n + \cdots}}}$ — *continued fraction*: here, $a_0 \in \mathbb{Z}$, $a_1, \ldots, a_n \in \mathbb{N}$, and the last term a_n, if it exists, is greater than 1.
- $\delta_k = [a_0, a_1, \ldots, a_k] = \frac{P_k}{Q_k}$, $k = 0, 1, \ldots, n, \ldots$ — the *convergants* of the continued fraction $[a_0, a_1, \ldots, a_n, \ldots]$.
- a_1, $a_2 = a_1 + d$, $a_3 = a_2 + d = a_1 + 2d$, $\ldots$, $a_n = a_{n-1} + d = a_1 + (n-1)d$, $\ldots$, where $a_1, d \in \mathbb{R}$ — *arithmetic progression* with *difference* d; $a_1 + \cdots + a_n = \frac{n(a_1 + a_n)}{2}$.
- b_1, $b_2 = b_1 \cdot q$, $b_3 = b_2 \cdot q = b_1 \cdot q^2$, $\ldots$, $b_n = b_{n-1} \cdot q = b_1 \cdot q^{n-1}$, $\ldots$, where $b_1, q \in \mathbb{R}\backslash\{0\}$ — *geometric progression* with *common ratio* q; $b_1 + \cdots + b_n = \frac{b_1(q^n - 1)}{q - 1}$ for $q \neq 1$.
- $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n + \cdots, |x| < r$ — *generating function* of the sequence $c_0, c_1, c_2, \ldots, c_n, \ldots$.
- $A = ((a_{ij}))$, $1 \leq i, j \leq n$ — square $n \times n$ matrix with real entries a_{ij}. The matrix A is called *symmetric*, if $a_{ij} = a_{ji}$ for all $i, j \in \{1, 2, \ldots, n\}$. The matrix A is called *identity matrix* and denoted by I_n, if $a_{ii} = 1$ and $a_{ij} = 0$ for $i \neq j$. The matrix $A^T = ((a_{ji}))$ is called *transpose* of A. The matrix A^{-1} such that $A \cdot A^{-1} = I_n$ is called *inverse* of A.
- $det\, A$ or $|A|$ — *determinant* of a given $n \times n$ matrix $A = ((a_{ij}))$. For $n = 2$, it holds that $det\, A = a_{11}a_{22} - a_{21}a_{12}$; for any $n \geq 3$, it holds that $det\, A = \sum_{j=1}^{n} (-1)^{1+j} a_{1j} \cdot det\, A_{1j}$, where A_{1j} is the $(n-1) \times (n-1)$ matrix, obtained by deletion of the first row and the jth column of A.
- $n!$ — *factorial* of a non-negative integer n: $n! = 1 \cdot 2 \cdot \ldots \cdot n$, $n \in \mathbb{N}$; $0! = 1$.

- $n\sharp$ — *primorial* of a positive integer n: the product of all primes less than or equal to n.
- $\binom{n}{m}$ — *binomial coefficients*; C_n^m — the number of *combinations*, i.e., the ways to choose an unordered subset of m elements from a fixed set of n elements; $\binom{n}{m} = C_n^m = \frac{n!}{m!(n-m)!}$, $0 \leq m \leq n$. They form the *Pascal's triangle*

$$\begin{array}{c}
\binom{0}{0} = 1 \\
\binom{1}{0} = 1 \quad \binom{1}{1} = 1 \\
\binom{2}{0} = 1 \quad \binom{2}{1} = 2 \quad \binom{2}{2} = 1 \\
\binom{3}{0} = 1 \quad \binom{3}{1} = 3 \quad \binom{3}{2} = 3 \quad \binom{3}{3} = 1 \\
\binom{4}{0} = 1 \quad \binom{4}{1} = 4 \quad \binom{4}{2} = 6 \quad \binom{4}{3} = 4 \quad \binom{4}{4} = 1 \\
\binom{5}{0} = 1 \quad \binom{5}{1} = 5 \quad \binom{5}{2} = 10 \quad \binom{5}{3} = 10 \quad \binom{5}{4} = 5 \quad \binom{5}{5} = 1 \\
\binom{6}{0} = 1 \quad \binom{6}{1} = 6 \quad \binom{6}{2} = 15 \quad \binom{6}{3} = 20 \quad \binom{6}{4} = 15 \quad \binom{6}{5} = 6 \quad \binom{6}{6} = 1 \\
\dots \quad \dots \quad \dots
\end{array}$$

  — number triangle, the sides of which are formed by 1, and any inner entry is obtained by adding the two entries diagonally above.
- $f(x) = O(g(x))$ — *big O notation*: for a complex-valued function f and a real-valued function g, $g(x) > 0$ for all large enough values of x, there exists a positive real number C and a real number x_0 such that $|f(x)| \leq C \cdot g(x)$ for all $x \geq x_0$.
- $f(x) = o(g(x))$ — *small o notation*: for a complex-valued function f and a real-valued function g, $g(x) > 0$ for all large enough values of x, $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$.
- $f(x) \sim g(x)$: for a complex-valued function f and a real-valued function g, $g(x) > 0$ for all large enough values of x, $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.
- $e = 2.718281828\dots$ — the *Euler's number*: $e = \lim_{n\to\infty}(1 + \frac{1}{n})^n$.
- $\gamma = 0.5772156649\dots$ — the *Euler–Mascheroni constant*: $\gamma = \lim_{n\to\infty}\left(\sum_{k=1}^{n} \frac{1}{k} - \log n\right)$.
- $\log x = \log x = \log_e x$ — *natural logarithm* of a positive real number x: its logarithm to the base e.
- $Li(n)$ — *logarithmic integral*: $Li(n) = \int_2^n \frac{dx}{\log x}$.

This page intentionally left blank

Contents

Preface vii

About the Author xv

Notations xvii

1. Preliminaries 1

1.1 Divisibility of Integers 1
1.2 Modular Arithmetic 8
1.3 Solution to Congruences 13
1.4 Quadratic Residues, Legendre Symbol, and Jacobi Symbol 19
1.5 Multiplicative Orders, Primitive Roots, and Indexes 22
1.6 Continued Fractions and Their Applications 25

2. Arithmetic Functions 35

2.1 Additive and Multiplicative Functions 35
2.2 Floor Function and Its Relatives 42
2.3 Möbius Function 46
2.4 Euler's Totient Function 50
2.5 Prime Counting Functions 59
2.6 Divisor Functions 86

3. Perfect Numbers 107

3.1 History of the Question 107
3.2 Divisor Function and Perfect Numbers 119
3.3 Properties of Perfect Numbers 132
3.4 Search for Perfect Numbers 155
3.5 Perfect Numbers in the Family of Special Numbers 176
3.6 Open Problems 217

4. Amicable Numbers 229

4.1 History of the Question 229
4.2 Divisor Function and Amicable Numbers 238
4.3 Properties of Amicable Numbers 258
4.4 Search for Amicable Numbers 268
4.5 Amicable Numbers in the Family of Special Numbers 280
4.6 Open Problems 289

5. Generalizations and Analogue 299

5.1 History of the Question 299
5.2 Relatives of Perfect Numbers 305
5.3 Relatives of Amicable Numbers 333
5.4 Sociable Numbers 345
5.5 Search for Numbers Under Consideration 354
5.6 Open Problems 365

6. Zoo of Numbers 371

7. Mini Dictionary 383

8. Exercises 393

Bibliography 419

Index 433

Chapter 1

Preliminaries

1.1. Divisibility of Integers

By positive integer (natural) numbers, we mean the numbers $1, 2, 3, \ldots$; by integers, we mean the positive integers, the number zero, and the negative integers: $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$.

Division algorithm

1.1.1. The *division algorithm* (or *integer division algorithm*) is a theorem in mathematics which precisely expresses the outcome of the usual process of division of integers.

Theorem (division algorithm). *For any $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.*

The number q is called the *quotient*, r is called the *remainder* and is denoted by $rest(a, b)$, b is called the *divisor*, and a is called the *dividend*.

For example, $-10 = 3 \cdot (-4) + 2$; $22 = 3 \cdot 7 + 1$; $100 = 20 \cdot 5 + 0$.

Divisibility

1.1.2. We say that *an integer a is divisible by an integer b, $b \neq 0$,* and write $b|a$, *if there is an integer c such that*

$$a = b \cdot c.$$

In this case, b is called a *divisor* of a and a is called a *multiple* of b.

For example, $2|10$, as $10 = 2 \cdot 5$; $(-6)|42$, as $42 = (-6) \cdot (-7)$; but $14 \not| 25$, as there exists no integer c such that $14 = 25 \cdot c$.

Divisors can be negative as well as positive, although often we restrict our attention to positive divisors.

The numbers 1 and -1 divide (are divisors of) every integer, every integer (except 0) is a divisor of itself, and every integer is a divisor of 0, except by convention 0 itself.

Numbers divisible by 2 are called *even*; numbers not divisible by 2 are called *odd*.

A divisor of n that is not 1, -1, n, or $-n$ is known as a *non-trivial divisor*.

For example, 6 is an even number, as it is divisible by 2; it has four trivial divisors ± 1, ± 6, and four non-trivial divisors, $\pm 2, \pm 3$; 3 is an odd number, as it is not divisible by 2; it has only trivial divisors, ± 1, ± 3; 2 is an even number; it has only trivial divisors, ± 1, ± 2; 1 is an odd number, as it is not divisible by 2; it has only trivial divisors, ± 1.

A positive divisor of n which is different from n is called a *proper divisor* (or *aliquot part*) of n.

For example, 6 has three proper divisors: 1, 2, and 3.

Properties of divisibility

1. If $a|b$ and $a|c$, then $a|(b + c)$; in fact, $a|(mb + nc)$ for all integers m and n.
2. If $a|b$ and $b|c$, then $a|c$.
3. If $a|b$ and $b|a$, then $a = b$, or $a = -b$.

For the proof of these properties and some additional information, see, for example, in [Buch09] and [DeKo13].

Prime and composite numbers

1.1.3. Positive integers with non-trivial divisors are known as *composite numbers*, while *prime numbers* have no non-trivial divisors.

Formally, a positive integer p is called *prime* if it has exactly two positive integer divisors (which are 1 and the prime number itself).

For example, 2 is a prime number, as it has exactly two positive divisors, 1 and 2; 3 is a prime number, as it has exactly two positive divisors, 1 and 3.

The first 30 prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, and 113 (see sequence A000040 in OEIS).

The property of being a prime is called *primality.*

A positive integer n is called *composite* if it has more than two positive integer divisors.

For example, 4 is a composite number, as it has three positive divisors, 1, 2, and 4; 6 is a composite number, as it has four positive divisors, 1, 2, 3, and 6; 15 is a composite number, as it has four positive divisors, 1, 3, 5, and 15.

The first 30 composite numbers are 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30 32, 33, 34, 35, 36, 38, 39, 40, 42, 44, and 45 (see the sequence A002808 in the OEIS).

The number 1 has exactly one positive divisor, 1 itself. It is the only positive integer which is neither prime nor composite.

So, any positive integer is either a prime number or composite number or is equal to 1.

Any composite number n can be represented as $n = a \cdot b$, where $1 < a \leq b < n$.

For example, $4 = 2 \cdot 2$; $6 = 2 \cdot 3$; $20 = 2 \cdot 10 = 4 \cdot 5$.

For any prime number, if $p = a \cdot b$, then $a, b \in \{\pm 1, \pm p\}$.

Any natural number n greater than one has a prime divisor; in fact, it is the smallest positive divisor of n greater than 1.

For example, $2|4$; $3|15$; $5|5$.

The *fundamental theorem of arithmetic* (or *unique factorization theorem*) states that *every positive integer larger than* 1 *can be written as a product of one or more primes in a unique way, i.e., unique except for the order.*

For example, $4 = 2^2$; $5 = 5$; $6 = 2 \cdot 3$; $600 = 2^3 \cdot 3 \cdot 5^2$.

For additional information, see, for example, [Buch09], [DeKo13], [Ribe89], and [Sier64].

Greatest common divisor and least common multiple

1.1.4. Given integers $a_1, \dots, a_n$, not all equal to zero, the *greatest common divisor* $gcd(a_1, \dots, a_n)$ of $a_1, \dots, a_n$ is defined as the largest positive integer that divides all numbers $a_1, \dots, a_n$.

For example, the set of divisors of the number 4 is $\{\pm 1, \pm 2, \pm 4\}$; the set of divisors of the number 6 is $\{\pm 1, \pm 2, \pm 3, \pm 6\}$; so, the set of common divisors of the numbers 4 and 6 is $\{\pm 1, \pm 2\}$, and $gcd(4, 6) = 2$.

Given non-zero integers $a_1, \dots, a_n$, the *least common multiple* $lcm(a_1, \dots, a_n)$ of $a_1, \dots, a_n$ is defined as the smallest positive integer that is a multiple of all numbers $a_1, \dots, a_n$.

For example, the set of multiples of the number 4 is $\{\pm 4, \pm 8, \pm 12, \pm 16, \pm 20, \pm 24, \dots\}$; the set of multiples of the number 6 is $\{\pm 6, \pm 12, \pm 18, \pm 24, \pm 30, \pm 36, \dots\}$; so, the set of common multiples of the numbers 4 and 6 is $\{\pm 12, \pm 24, \pm 36, \dots\}$, and $lcm(4, 6) = 12$.

Properties of *gcd* and *lcm*

1. $gcd(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}, p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}) = p_1^{\gamma_1} \cdot \ldots \cdot p_k^{\gamma_k}$, where $\alpha_i, \beta_i \geq 0$, and $\gamma_i = \max\{\alpha_i, \beta_i\}$, $i = 1, 2, \dots, k$.
2. $lcm(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}, p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}) = p_1^{\delta_1} \cdot \ldots \cdot p_k^{\delta_k}$, where $\alpha_i, \beta_i \geq 0$, and $\delta_i = \min\{\alpha_i, \beta_i\}$, $i = 1, 2, \dots, k$.
3. Every common divisor of a and b is a divisor of $gcd(a, b)$.
4. If $gcd(a, b) = d$, then there exist integers x and y such that $ax + by = d$ (*Bézout's identity*).
5. If $a|bc$ and $gcd(a, b) = d$, then $\frac{a}{d}|c$.
6. $gcd(m \cdot a, m \cdot b) = m \cdot gcd(a, b)$ for any $m \in \mathbb{N}$.
7. $gcd(a + m \cdot b, b) = gcd(a, b)$ for any $m \in \mathbb{Z}$.
8. If $m|a$ and $m|b$, where $m \in \mathbb{N}$, then $gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{gcd(a,b)}{m}$.
9. $gcd(a, b) \cdot lcm(a, b) = a \cdot b$ for any positive integers a and b.

It is useful to define $gcd(0,\ 0) = 0$ and $lcm(0,\ 0) = 0$ because the set of natural numbers then becomes a complete distributive lattice with *gcd* as meet or with *lcm* as join operation.

The greatest common divisor can more generally be defined for elements of an arbitrary commutative ring.

For a proof of these properties and for some additional information see, for example, [Buch09], [DeKo13], and [Kost82].

Euclidean algorithm

1.1.5. The *Euclidean algorithm* (also called *Euclid's algorithm*) is an algorithm to determine the greatest common divisor of two integers by repeatedly dividing the two numbers and the remainders in turns.

Theorem (Euclidean algorithm). *For any integer a and any natural number b which does not divide a, the greatest common divisor of a and b is equal to the last non-zero reminder r_s in the following algorithm*:

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1 q_2 + r_2, \\ &\vdots \\ r_{s-2} &= r_{s-1} q_s + r_s, \\ r_{s-1} &= r_s q_s + 0, \end{aligned}$$

where $r_1 > r_2 > \cdots > r_s > 0$.

For example, as

$$\begin{aligned} 1071 &= 1029 \cdot 1 + 42, \\ 1029 &= 42 \cdot 24 + 21, \\ 42 &= 21 \cdot 2 + 0, \end{aligned}$$

we obtain that $gcd(1071, 1029) = 21$.

The Euclidean algorithm is one of the oldest known algorithms since it appeared in Euclid's *Elements* around 300 BC. Euclid originally formulated the problem geometrically, as the problem of finding a common "measure" for two line lengths, and his algorithm proceeded by repeated subtraction of the shorter from the longer segment.

However, the algorithm was probably not discovered by Euclid, and it may have been known up to 200 years earlier. It was almost certainly known by Eudoxus of Cnidus (about 375 BC); Aristotle (about 330 BC) hinted at it in his *Topics*.

This algorithm can be used in any context where division with remainder is possible. This includes rings of polynomials over a field as well as the ring of Gaussian integers and, in general, all Euclidean domains.

For a proof of the theorem and for some additional information see, for example, [Buch09], [DeKo13], [DeKo18], [Kost82], and [Stra16].

Coprime numbers

1.1.6. Two integers a and b are called *coprime* (or *relatively prime*) if their greatest common divisor is equal to 1, i.e., they have no common factors other than 1 and -1.

For example, 6 and 35 are coprime, as $gcd(6, 35) = 1$, but 6 and 27 are not because $gcd(6, 27) = 3$.

The number 1 is coprime to every integer; 0 is coprime only to 1 and -1.

Properties of coprime numbers

1. a and b are coprime if and only if there exist integers x and y such that $ax + by = 1$.
2. If $b|ac$ and $gcd(b, c) = 1$, then $b|a$.
3. If $b|a, c|a$ and $gcd(b, c) = 1$, then $bc|a$.
4. $gcd(a, b) = 1$ if and only if $gcd(a^n, b^m) = 1$ for any non-negative integers m and n.

The first property gives a criterion of coprime numbers, see *Bézout's identity*. The second property can be viewed as a generalization of *Euclid's lemma*, which states that if p is a prime and $p|bc$, then either $p|b$ or $p|c$.

In fact, we can easily check all the properties of coprime numbers using the fundamental theorem of arithmetic, as two coprime numbers have no common prime divisors.

For a proof of these properties and for some additional information, see, for example, [Arno38], [BiBa70], [Buch09], [CoGu96], [DeKo13], [DeKo18], [Dick05], [Gelf98], [IrRo90], [Knut68], [Kost82], [Lege79], [Moze09], [Ore48], [Stra16], and [Wiki22].

Exercises

1. Prove that any integer number can be represented as:
   (a) $6k$, or $6k \pm 1$, or $6k \pm 2$, or $6k + 3$, $k \in \mathbb{Z}$;
   (b) $7k$, or $7k \pm 1$, or $7k \pm 2$, or $7k \pm 3$, $k \in \mathbb{Z}$;
   (c) $10k$, or $10k \pm 1$, or $10k \pm 2$, or $10k \pm 3$, or $10k \pm 4$, or $10k + 5$, $k \in \mathbb{Z}$;
   (d) $12k$, or $12k \pm 1$, or $12k \pm 2$, or $12k \pm 3$, or $12k \pm 4$, or $12k \pm 5$, or $12k + 6$, $k \in \mathbb{Z}$.
2. Prove that a perfect square cannot be represented as:
   (a) $3k - 1$;
   (b) $4k - 1$;
   (c) $5k + 2$;
   (d) $5k - 2$;
   (e) $6k + 2$;
   (f) $6k - 1$.
3. Prove that $a^2 + b^2 \neq c^2$ for any odd integers a and b.
4. Prove that $a^2 + b^2 \neq c^3$ for any odd integers a and b.
5. Prove that for any integer a, the following holds:
   (a) $a^{10} - 9a + 8$ is divisible by 2;
   (b) $a^5 + 3a^3 - 12$ is divisible by 4;
   (c) $a^3 - 7a + 18$ is divisible by 6;
   (d) $a^7 - a - 56$ is divisible by 7;
   (e) $a^5 - 17a^3 + 24$ is divisible by 8;
   (f) $a^7 + 17a - 18$ is divisible by 9.
6. Prove that $n \cdot (n^2 + 1) \cdot (n^2 + 4)$ is divisible by 5 for any integer n.
7. Prove that $5^{2n+1} \cdot 2^{n+2} + 3^{n+2} \cdot 2^{2n+1}$ is divisible by 19 for any $n \geq 0$.
8. Find the greatest common divisor of 11111111 and $\underbrace{111\ldots\ldots.111}_{100 \text{ unities}}$.

9. For any positive integer n, find greatest common divisor of:
   (a) $n^3 + 11n$ and 6;
   (b) $(n^2 - 1) \cdot n^2 \cdot (n^2 + 1)$ and 60;
   (c) $n^5 + 4n$ and 10;
   (d) $n^5 - 5n^4 + 4n$ and 10.

10. Prove that for any positive integer n, the following holds:
   (a) $n^6 - n$ is divisible by 60;
   (b) $n^7 - n^3$ is divisible by 120;
   (c) $10^n + 5$ is divisible by 15;
   (d) $7^{6n} - 1$ is divisible by 18.

1.2. Modular Arithmetic

Congruence relation

1.2.1. *Modular arithmetic* (sometimes called *modulo arithmetic*) is a system of arithmetic for integers where numbers "wrap around" after they reach a certain value — the *modulus*. Modular arithmetic was introduced by C. F. Gauss in his book *Disquisitiones Arithmeticae*, published in 1801.

Two integers a and b are called *congruent modulo* n, $n \in \mathbb{N}$, if a and b have the same remainder when divided by n or, equivalently, if $n|(a - b)$. In this case, it is expressed as

$$a \equiv b(mod\ n).$$

For example, $6 \equiv 22(mod\ 4)$, as $4|(22 - 6)$; $2 \equiv -7(mod\ 3)$, as $3|(2 - (-7))$; but $5 \not\equiv 12(mod\ 6)$, as $6 \not| (5 - 12)$.

Properties of congruence relation

1. $a \equiv a(mod\ n)$ (*reflexivity*).
2. If $a \equiv b(mod\ n)$, then $b \equiv a(mod\ n)$ (*symmetry*).
3. If $a \equiv b(mod\ n)$ and $b \equiv c(mod\ n)$, then $a \equiv c(mod\ n)$ (*transitivity*).

4. If $a \equiv b(mod\ n)$, then $f(a) \equiv f(b)(mod\ n)$, where $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ is a polynomial with integer coefficients $a_m, \ldots, a_1, a_0$.
5. $a \equiv b(mod\ n)$ if and only if $k \cdot a \equiv k \cdot b(mod\ k \cdot n)$ for any positive integer k.
6. $a \equiv b(mod\ n)$ if and only if $k \cdot a \equiv k \cdot b(mod\ n)$ for any integer k such that $gcd(k, n) = 1$.
7. $a \equiv b(mod\ n_i)$, $i = 1, \ldots, k$, if and only if $a \equiv b(mod\ M)$, where $M = lcm(n_1, \ldots, n_k)$.

It is easy to see from properties 1, 2, and 3 that the congruence relation $\equiv$ modulo n is an *equivalence relation* on the set $\mathbb{Z}$ of integers.

For the proof of these properties and for some additional information, see, for example, in [Buch09], [DeKo13], and [Gaus01].

Congruence classes

1.2.2. The set

$$\begin{aligned}[a]_n &= \{x \in \mathbb{Z} : x \equiv a(mod\ n)\} \\ &= \{\ldots, a-3n, a-2n, a-n, a, a+n, a+2n, a+3n, \ldots\}\end{aligned}$$

of all integers congruent to a given number a modulo n is called the *congruence class* (or *residue class*) *of a modulo n*.

The smallest non-negative representative of $[a]_n$ is called *smallest non-negative residue* of a modulo n; it is the reminder $rest(a, n)$ of a after its integer division by n. The smallest in absolute value representative of $[a]_n$ is called *minimal residue* of a modulo n.

For example,

$$\begin{aligned}[2]_5 &= \{x \in \mathbb{Z} : x \equiv 2(mod\ 5)\} \\ &= \{\ldots, 2-3\cdot 5, 2-2\cdot 5, 2-5, 2, 2+5, 2+2\cdot 5, 2+3\cdot 5, \ldots\} \\ &= \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}.\end{aligned}$$

The smallest non-negative residue of the class $[2]_5$, as well as its minimal residue, is 2. On the other hand,

$[19]_5 = \{x \in \mathbb{Z} : x \equiv 19(mod\ 5)\} = \{\ldots, -6, -1, 4, 9, 14, 19, , 24, \ldots\}$.

The smallest non-negative residue of the class $[19]_5$ is 4, while its minimal residue is -1.

Properties of residue classes modulo n

1. $[a]_n = \{a + mt : t \in \mathbb{Z}\}$.
2. $[a]_n = [b]_n$ if and only if $a \equiv b(mod\ n)$.
3. There are exactly n residue classes modulo n.
4. If $x \in [a]_n$, then $gcd(x, n) = gcd(a, n)$.
5. A residue class $[a]_n$ modulo n gives k residue classes $[a]_{kn}$, $[a+n]_{kn}$, $[a + 2n]_{kn}, \ldots, [a + (k - 1)n]_{kn}$ modulo kn, $k \in \mathbb{N}$.

One can define an addition and multiplication on the set

$$Z/nZ = \{[0]_n, [1]_n, [2]_n, \ldots, [n - 1]_n\}$$

of all equivalence classes modulo n by the following rules:

$$[a]_n + [b]_n = [a + b]_n \quad \text{and} \quad [a]_n \cdot [b]_n = [a \cdot b]_n.$$

In this way, Z/nZ becomes a commutative ring $(Z/nZ, +, \cdot)$ with n elements. For a prime number p, the ring $(Z/pZ, +, \cdot)$ forms a field.

Fermat's little theorem and Euler's theorem

1.2.3. A complex-valued function $f(n)$ is called *arithmetic function* if the value $f(n)$ is determined for any positive integer n.

An arithmetic function f is called *multiplicative* if $f(1) = 1$ and

$$f(m \cdot n) = f(m) \cdot f(n)$$

for any coprime positive integers n and m.

An multiplicative function f is called *completely multiplicative* if the condition $f(m \cdot n) = f(m) \cdot f(n)$ holds for any positive integers m and n.

For example, the function $f(n) = n^\alpha$ is completely multiplicative for any real number α. The divisor function, the Möbius function, and the Euler's totient function are multiplicative but not completely multiplicative. The prime counting function $\pi(x)$ is not a multiplicative function.

1.2.4. Given a positive integer n, the *Euler's totient function* $\phi(n)$ is defined as the number of positive integers less than or equal to n

and coprime to n:

$$\phi(n) = |\{x \in \mathbb{N} : x \leq n, gcd(x, n) = 1\}|.$$

For example, $\phi(8) = 4$ since exactly four numbers, 1, 3, 5, and 7, less than or equal to 8, are coprime to 8.

The function ϕ is usually called the *Euler's totient* (or *Euler totient*) after L. Euler who studied it. The totient function is also called *Euler's phi function*, or simply *phi function*, since the letter ϕ is so commonly used for it.

Properties of Euler's totient function

1. $\phi(p) = p - 1$ for any prime p.
2. $\phi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$, for any prime p and any positive integer α.
3. The Euler's totient function is multiplicative, i.e., $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$ for any coprime positive integers m and n.
4. $\phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot (p_s^{\alpha_s}) = (p_1^{\alpha_1} - p^{\alpha_1 - 1})(p_2^{\alpha_2} - p^{\alpha_2 - 1}) \cdot \ldots \cdot p_s^{\alpha_s} - p_s^{\alpha_s - 1})$ for any primes $p_1 < p_2 < \cdots < p_s$ and any positive integers $\alpha_1, \alpha_2, \ldots, \alpha_s$.

The Euler's totient function is important mainly because it gives the size of the multiplicative group of integers modulo n. More precisely, $\phi(n)$ is the order of the group of units of the ring $(Z/nZ, +, \cdot)$.

1.2.5. Now, we consider two important theorems: the Fermat's little theorem and its generalization the *Euler's theorem*.

Theorem (Fermat's little theorem). *If p is a prime number, then, for any integer a,*

$$a^p \equiv a(mod\ p).$$

It means that if you start with a number, initialized to 1, and repeatedly multiply, for a total of p multiplications, $p \in P$, that number by a, $a \in \mathbb{Z}$, and then subtract a from the resulting number, the final result will be divisible by p.

A variant of this theorem is stated in the following form: *if p is a prime and a is an integer coprime to p, then*

$$a^{p-1} \equiv 1(mod\ p).$$

In other words, if p is a prime number and a is any integer that does not have p as a factor, then a raised to the $(p-1)$th power will leave a remainder of 1 when divided by p.

Fermat's little theorem is the basis for the *Fermat primality test* (see Chapter 2, Section 2.3).

1.2.6. The *Euler's theorem* (also known as the *Fermat–Euler theorem* or *Euler's totient theorem*) is a generalization of Fermat's little theorem. L. Euler published a proof of this theorem in 1736.

Theorem (Euler's theorem). *If n is a positive integer and a is an integer coprime to n, then*

$$a^{\phi(n)} \equiv 1 (mod\ n).$$

Here, $\phi(n)$ is Euler's totient function.

The Euler's theorem may be used to easily reduce large powers modulo n.

1.2.7. The Euler's theorem is further generalized by the *Carmichael's theorem.*

Theorem (Carmichael's theorem). *If n is a positive integer and a is an integer coprime to n, then*

$$a^{\lambda(n)} \equiv 1 (mod\ n).$$

Here, $\lambda(n)$ is the *Carmichael function*, defined recursively:

- for prime $p \geq 3$ and positive integer α, $\lambda(p^\alpha) = \phi(p^\alpha)$;
- for positive integer $\alpha \geq 3$, $\lambda(2^\alpha) = 2^{\alpha-2}$, while $\lambda(2) = 1$ and $\lambda(4) = 2$;
- and finally, $\lambda(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}) = lcm(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_k^{\alpha_k}))$.

For the proofs of these theorems and for some additional information, see, for example, [Buch09], [DeKo13]. [DeKo18], [Dick05], [IrRo90], [Lege79], [Moze09], [Ore48], [Sier64], [Step01], [Stra16], and [Wiki22].

Exercises

1. Is the congruence $10! \equiv 7! (mod\ 1000)$ true?
2. Is the congruence $\binom{14}{7} \equiv \binom{10}{5} (mod\ 5710)$ true?
3. Find $rest(f(86), 11)$ if $f(x) = 15x^3 - 33x^2 + 7$.
4. Find the smallest four-digit positive integer congruent to 23 modulo 101; modulo 100; and modulo 99.

5. Prove that $9^{2n+1} + 8^{n+2} \equiv 0(mod\ 73)$ for any $n \geq 0$.
6. For what value of n, the following holds:
   (a) $51 \cdot 52 \cdot \ldots \cdot 300 \equiv 0(mod\ 11^n)$;
   (b) $51 \cdot 52 \cdot \ldots \cdot 300 \equiv 0(mod\ 15^n)$;
   (c) $31 \cdot 32 \cdot \ldots \cdot 400 \equiv 0(mod\ 7^n)$;
   (d) $31 \cdot 32 \cdot \ldots \cdot 400 \equiv 0(mod\ 33^n)$?
7. Check that:
   (a) $[73]_5 = [-92]_5$;
   (b) $[99]_6 = [-87]_6$;
   (c) $[3!]_8 = [-2!]_8$;
   (d) $[12!]_9 = [15!]_9$.
8. Find the result of the calculation:
   (a) $[2]_{12} \cdot [9]_{12} + 2 \cdot [5]_{12}$;
   (b) $3 \cdot [4]_{14} \cdot [4]_{14} - 7 \cdot [9]_{14}$;
   (c) $34 \cdot [4]_{17} \div [2]_{17} + 5 \cdot ([4]_{17})^2$;
   (d) $2 \cdot ([5]_{23})^3 - [18]_{23} - 69 \cdot [5]_{23} \div [3]_{23}$.
9. Find the reminder of the division:
   (a) 5^{14} by 7;
   (b) 24^{16} by 7;
   (c) 5^{100} by 11;
   (d) 15^{175} by 11;
   (e) 3^{100} by 16;
   (f) 37^{100} by 16;
   (g) 3^{20} by 28;
   (h) 31^{200} by 28.
10. Is it true that for $f(x) = 292x^{181} - 121x^{133} + 252x^{122} - 171x^{121} - 133x^{62} + 3$, the following holds:
    (a) $f(24) \equiv -2(mod\ 13)$;
    (b) $f(-24) \equiv 2(mod\ 11)$;
    (c) $f(-55) \equiv -4(mod\ 13)$;
    (d) $f(55) \equiv 4(mod\ 11)$?
11. Find $rest(10^{100^{100}}, 71)$.

1.3. Solution to Congruences

1.3.1. Let $f(x) = a_m x^m + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients and $a_m \not\equiv 0(mod\ n)$. If, for some $x_0 \in \mathbb{Z}$, $f(x_0) \equiv 0(mod\ n)$, then for any $y \equiv x_0(mod\ n)$, one has also that $f(y) \equiv 0(mod\ n)$, and we say that the residue class $[x_0]_n$, i.e., the class $x \equiv x_0(mod\ n)$, is a solution to the congruence $f(x) \equiv 0(mod\ n)$, which is called a *congruence of order m modulo n.*

Linear congruences

1.3.2. The *linear congruence theorem* states that *the linear congruence* $ax + b \equiv 0(mod\ n)$ *has exactly one solution if* $gcd(a, n) = 1$, *exactly* d *solutions if* $gcd(a, n) = d$, $d|n$, *and no solutions otherwise.*

Theorem (linear congruence theorem).

- *If* $gcd(a, n) = 1$, *the linear congruence* $ax + b \equiv 0(mod\ n)$ *has exactly one solution,* $x \equiv x_0(mod\ n)$;
- *If* $gcd(a, n) = d$, $d|n$, *the linear congruence* $ax + b \equiv 0(mod\ n)$ *has exactly* d *solutions,* $x \equiv x_0 + k \cdot \frac{n}{d}(mod\ n)$, $k = 0, .., d - 1$, *where* $x \equiv x_0(mod\ \frac{n}{d})$ *is the only solution to the linear congruence* $\frac{a}{d}x + \frac{b}{d} \equiv 0(mod\ \frac{n}{d})$;
- *If* $gcd(a, n) = d$, $d \not| n$, *the linear congruence* $ax + b \equiv 0(mod\ n)$ *has no solutions.*

The only solution $x \equiv x_0(mod\ n)$ to a linear congruence $ax + b \equiv 0(mod\ n)$, $gcd(a, n) = 1$, can be found:

- by consideration of all representatives $0, \dots, n - 1$ of the residue classes modulo n;
- by the formula $x_0 \equiv -b \cdot a^{\phi(n)-1}(mod\ n)$;
- by consideration of congruences $x_0 \equiv \frac{-b+kn}{a}(mod\ n)$, $k = 0, 1, \dots, a - 1$, etc.

For example, a linear congruence

$$11x - 5 \equiv 0(mod\ 7)$$

has the only solution (a residue class modulo 7), as $gcd(11, 7) = 1$. It is equivalent to the congruence $4x \equiv -2(mod\ 7)$.

Checking the numbers $0, 1, 2, \dots, 6$, we obtain that $4 \cdot 3 \equiv -2(mod\ 7)$, i.e., the only solution to the congruence $4x \equiv -2(mod\ 7)$ is the residue class $x \equiv 3(mod\ 7)$.

On the other hand, using the formula

$$4x \equiv -2 + 7k(mod\ 7)$$

for $k = 0, 1, 2 \dots$, we obtain

$$4x \equiv -2(mod\ 7),\ 4x \equiv 5(mod\ 7), \text{and } 4x \equiv 12(mod\ 7).$$

Dividing the two sides of the last congruence by 4, we obtain that $x \equiv 3(mod\ 7)$.

Finally, using the Euler's totient function and the fact that $4^{\phi(7)-1} = 4^5$, we get the following congruence:

$$x \equiv -2 \cdot 4^5 (mod\ 7).$$

As

$$4^5 \equiv (-3)^5 \equiv 9 \cdot (-27) \equiv 2 \cdot 1 \equiv 2(mod\ 7),$$

we get that $x \equiv -2 \cdot 2 \equiv -4 \equiv 3(mod\ 7)$.

For the proof of this theorem and for some additional information, see, for example, [Buch09] and [DeKo13].

Chinese remainder theorem

1.3.3. The *Chinese remainder theorem* states that *the system of linear congruences with pairwise coprime modules n_i has exactly one solution, a residue class modulo $N = lcm(n_1, \ldots, n_k) = n_1 \cdot \ldots \cdot n_k$.*

Theorem (Chinese remainder theorem). The system of linear congruences

$$\begin{cases} x \equiv c_1 (mod\ n_1) \\ \vdots \\ x \equiv c_k (mod\ n_k) \end{cases}$$

with pairwise coprime modules $n_1, \ldots, n_k$ has exactly one solution, i.e., the residue class modulo

$$N = lcm(n_1, \ldots, n_k) = n_1 \cdot \ldots \cdot n_k,$$

which has the form

$$x \equiv \frac{N}{n_1} c_1 y_1 + \cdots + \frac{N}{n_k} c_k y_k (mod\ N),$$

where y_i is a solution to the linear congruence, $\frac{N}{n_i} y \equiv 1(mod\ n_i)$.

For example, consider a system of linear congruences:

$$\begin{cases} x \equiv 4\ \ (mod\ 5) \\ x \equiv 1\ (mod\ 12) \\ x \equiv 0\ \ (mod\ 7). \end{cases}$$

It is easy to see that

$$lcm(5, 12, 7) = lcm(5, 2^2 \cdot 3, 7) = 2^2 \cdot 3 \cdot 5 \cdot 7 = 420.$$

As $x \equiv 1(mod\ 12)$, we get $x = 12t + 1$, where $t \in \mathbb{Z}$.

Using the representation $x = 12t + 1$ in the congruence $x \equiv 0(mod\ 7)$, we get a new congruence $12t + 1 \equiv 0(mod\ 7)$ with argument t. It is easy to see that $-2t \equiv -1(mod\ 7)$, or $-2t \equiv 6(mod\ 7)$, or $t \equiv -3(mod\ 7)$. So, $t = 7t_1 - 3$, where $t_1 \in \mathbb{Z}$, i.e., $x = 12(7t_1 - 3) + 1 = 84t_1 - 35$, $t_1 \in \mathbb{Z}$.

Using the representation $x = 84t_1 - 35$ in the congruence $x \equiv 4(mod\ 5)$, we get $84t_1 - 35 \equiv 4(mod\ 5)$ with argument t_1. It is easy to see that $4t_1 \equiv 4(mod\ 5)$, or $t_1 \equiv 1(mod\ 5)$. So, $t_1 = 5t_2 + 1$, $t_2 \in \mathbb{Z}$, i.e., $x = 84(5t_2 + 1) - 35 = 420t_2 + 49,\ t_2 \in \mathbb{Z}$.

We obtain that the only solution to our system is the residue class $x \equiv 49(mod\ 420)$.

The original form of the theorem, contained in the third-century-book *Sun-tzu Suan-ching* by a Chinese mathematician Sun Tzu and later (1247) republished by Qin Jiushao, is a statement about simultaneous congruences; the general form of the Chinese remainder theorem can be formulated for rings and (two-sided) ideals.

For the proof of the theorem and for some additional information, see, for example, [Buch09], [DeKo13], [Dick05], [Kost82], and [Ore48].

Congruences of order m

1.3.4. Here, we consider a general algorithm of a solution to any congruence of order m, $m > 1$, composite modulo n.

I. Given a prime p, the congruence

$$f(x) \equiv 0(mod\ p)$$

of order m modulo p is equivalent to some congruence $x^s + \cdots + b_1x + b_0 \equiv 0(mod\ p)$ of order $s \leq p - 1$ modulo n and has at most s solutions.

One can find them by considering all representatives $0, \ldots, p-1$ of the residue class modulo p.

II. Given a prime p and a positive integer $\alpha > 1$, consider the congruence

$$f(x) \equiv 0(mod\ p^{\alpha})$$

of order m modulo p^α. We can use the following algorithm to find all the solutions to this congruence:

- Consider the congruence $f(x) \equiv 0(mod\ p)$, find all its solutions; let $x \equiv x_1(mod\ p)$ be one of these solutions, i.e., $f(x_1) \equiv 0(mod\ p)$ and $x = x_1 + pt_1$, $t_1 \in \mathbb{Z}$.
- Consider the linear congruence $\frac{f(x_1)}{p} + f^{'}(x_1)t_1 \equiv 0(mod\ p)$, find all its solutions; let $t_1 \equiv t^{'}(mod\ p)$ be one of these solutions, i.e., $t_1 = t^{'} + pt_2$ and $x = x_2 + p^2 t_2$.
- Consider the linear congruence $\frac{f(x_2)}{p^2} + f^{'}(x_2)t_2 \equiv 0(mod\ p)$, find all its solutions; let $t_2 \equiv t^{''}(mod\ p)$ be one of these solutions, i.e., $t_2 = t^{''} + pt_3$ and $x = x_3 + p^3 t_3$.

$$\vdots$$

- Consider the linear congruence $\frac{f(x_{\alpha-1})}{p^{\alpha-1}} + f^{'}(x_{\alpha-1})t_{\alpha-1} \equiv 0(mod\ p)$, find all its solutions; let $t_{\alpha-1} \equiv t^{''\cdots'}(mod\ p)$ be one of these solutions, i.e., $t_{\alpha-1} = t^{''\cdots'} + pt_\alpha$ and $x = x_\alpha + p^\alpha t_\alpha$.

Therefore, $x \equiv x_\alpha(mod\ p^\alpha)$ is one of the solutions of the congruence above, and all its solutions can be found in this way.

III. Lastly, for a given composite number $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, all the solutions of the congruence

$$f(x) \equiv 0(mod\ n)$$

of order m modulo n can be found using the following property: $f(x) \equiv 0(mod\ n)$ if and only if

$$\begin{cases} f(x) \equiv 0(mod\ p^{\alpha_1}) \\ \quad\vdots \\ f(x) \equiv 0(mod\ p_k^{\alpha_k}). \end{cases}$$

For the full explanation of the algorithm above and for many examples, you can see [Buch09] and [DeKo13]. For some additional information, see, for example, in [Arno38], [BiBa70], [Dick05], [Gaus01], [IrRo90], [Lege79], [Moze09], [Ore48], [Stra16] and [Wiki22].

Exercises

1. Solve the congruence:

   (a) $3x \equiv 1(mod\ 7)$;
   (b) $100x \equiv 21(mod\ 23)$;
   (c) $42x \equiv 33(mod\ 90)$;
   (d) $20x \equiv 12(mod\ 48)$;
   (e) $20x - 50 \equiv 0(mod\ 35)$;
   (f) $78x \equiv 102(mod\ 273)$;
   (g) $315x \equiv -10(mod\ 275)$;
   (h) $76x \equiv 232(mod\ 220)$;
   (i) $45x \equiv 75(mod\ 100)$.

2. Solve the system of congruences:

   (a) $\begin{cases} x \equiv 1(mod\ 5) \\ x \equiv 2(mod\ 6) \\ x \equiv 3(mod\ 7); \end{cases}$

   (b) $\begin{cases} 3x \equiv 7(mod\ 10) \\ 2x \equiv 5(mod\ 15) \\ 7x \equiv 5(mod\ 12); \end{cases}$

   (c) $\begin{cases} 5x + 7 \equiv 0(mod\ 12) \\ 3x \equiv 7(mod\ 8); \end{cases}$

   (d) $\begin{cases} 4x \equiv 3(mod\ 7) \\ 5x \equiv 4(mod\ 11) \\ 11x \equiv 8(mod\ 13); \end{cases}$

   (e) $\begin{cases} 18x \equiv 226(mod\ 10) \\ 30x \equiv 232(mod\ 24); \end{cases}$

   (f) $\begin{cases} 3x \equiv 1(mod\ 10) \\ 4x \equiv 3(mod\ 5) \\ 2x \equiv 7(mod\ 9); \end{cases}$

   (g) $\begin{cases} 5x \equiv 1(mod\ 12) \\ 5x \equiv 2(mod\ 8) \\ 7x \equiv 3(mod\ 11); \end{cases}$

   (h) $\begin{cases} 3x \equiv 5(mod\ 2) \\ x \equiv -3(mod\ 5) \\ 4x \equiv 7(mod\ 9); \end{cases}$

   (i) $\begin{cases} 20x \equiv -10(mod\ 15) \\ 2x \equiv -12(mod\ 10). \end{cases}$

3. Solve the congruence:

   (a) $x^3 + x^2 - 2x + 1 \equiv 0(mod\ 5)$;
   (b) $133x^5 - 148x^4 + 85x^3 - 98x^2 + x + 6 \equiv 0(mod\ 7)$;
   (c) $232x^{484} + 852x^{252} - 124x^{202} - x^{200} + 78 \equiv 0(mod\ 11)$;
   (d) $292x^{181} - 121x^{133} + 252x^{122} - 171x^{121} - 133x^{62} + 5 \equiv 0(mod\ 13)$;
   (e) $357x^{427} - 811x^{403} - 127x^{311} + 45 \equiv 0(mod\ 7)$;
   (f) $883x^{693} - 106x^{484} + 59x^{241} + 87x^{233} + 84 \equiv 0(mod\ 5)$;
   (g) $4015x^{10892} + 605x^{9999} + 365x^{1002} + 888x^{1001} - 24 \equiv 0(mod\ 11)$.

4. Solve the congruence:

   (a) $31x^4 + 57x^3 + 96x + 191 \equiv 0(mod\ 675)$;
   (b) $3x^4 - 8x^3 + 8x^2 - 3x + 3 \equiv 0(mod\ 225)$;

(c) $x^3 + 6x + 7 \equiv 0(mod\ 675)$;
(d) $x^3 + 2x^2 + 2x + 4 \equiv 0(mod\ 675)$;
(e) $x^3 - x^2 + x + 3 \equiv 0(mod\ 108)$;
(f) $x^3 + 5x^2 + 9x + 9 \equiv 0(mod\ 108)$.

1.4. Quadratic Residues, Legendre Symbol, and Jacobi Symbol

Given an odd prime p, an integer a coprime to p is called a *quadratic residue* modulo p if

$$x_0^2 \equiv a(mod\ p)$$

for some integer x_0. Otherwise, a is called quadratic nonresidue.

Legendre symbol

1.4.1. For any integer a coprime to an odd prime p, the *Legendre symbol* (named after A.-M. Legendre) $(\frac{a}{p})$ is defined by $\left(\frac{a}{p}\right) = 1$ if a is a quadratic residue modulo p and by $(\frac{a}{p}) = -1$ if a is a quadratic nonresidue modulo p. If $p|a$, one has $(\frac{a}{p}) = 0$.

Properties of Legendre symbol

1. $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}(mod\ p)$ (*Euler's criterion*).
2. If $a \equiv b(mod\ p)$, then $(\frac{a}{p}) = (\frac{b}{p})$.
3. $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.
4. $(\frac{a^2}{p}) = 1$; in particular, $(\frac{1}{p}) = 1$.
5. $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$, i.e., $(\frac{-1}{p}) = 1$ if $p \equiv 1(mod\ 4)$, and $(\frac{-1}{p}) = -1$ if $p \equiv -1(mod\ 4)$.
6. $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$, i.e., $(\frac{2}{p}) = 1$ if $p \equiv \pm 1(mod\ 8)$, and $(\frac{2}{p}) = -1$ if $p \equiv \pm 3(mod\ 8)$.
7. For distinct odd primes p and q,

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right),$$

i.e., $(\frac{p}{q}) = (\frac{q}{p})$ if $p \equiv 1(mod\ 4)$ or $q \equiv 1(mod\ 4)$, and $(\frac{p}{q}) = -(\frac{q}{p})$ if $p \equiv -1(mod\ 4)$ and $q \equiv -1(mod\ 4)$ (*law of quadratic reciprocity*).

For example,

$$\begin{aligned}\left(\frac{-125}{47}\right) &= \left(\frac{-5\cdot 25}{47}\right) = \left(\frac{-5}{47}\right)\cdot\left(\frac{5^2}{47}\right) = \left(\frac{-5}{47}\right)\\ &= \left(\frac{-1}{47}\right)\left(\frac{5}{47}\right) = (-1)\cdot\left(\frac{5}{47}\right)\\ &= (-1)\cdot\left(\frac{47}{5}\right) = (-1)\cdot\left(\frac{2}{5}\right) = (-1)\cdot(-1) = 1.\end{aligned}$$

It means that -125 is a quadratic residue modulo 47.

Jacobi symbol

1.4.2. The *Jacobi symbol* is a generalization of the Legendre symbol. (Another generalization is the *Kronecker symbol.* Additionally, the Legendre symbol is a *Dirichlet character.*)

Introduced by C. G. J. Jacobi in 1837, it is of theoretical interest in modular arithmetic and other branches of number theory, but its main use is in computational number theory, especially in primality testing and integer factorization.

For any integer a and any positive odd integer n, the *Jacobi symbol* $\left(\frac{a}{n}\right)$ is defined as the product of the Legendre symbols corresponding to the prime factors of n: for $n = p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k}$, it holds

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\cdot\ldots\cdot\left(\frac{a}{p_k}\right)^{\alpha_k}.$$

Like the Legendre symbol, if $\left(\frac{a}{n}\right) = -1$, then a is a quadratic nonresidue modulo n.

But, unlike the Legendre symbol, if $\left(\frac{a}{n}\right) = 1$, then a may or may not be a quadratic residue modulo n.

Properties of Jacobi symbol

1. If $a \equiv b(mod\ n)$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$;
3. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.
4. $\left(\frac{a^2}{n}\right) = 1$; in particular, $\left(\frac{1}{n}\right) = 1$.
5. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$, i.e., $\left(\frac{-1}{n}\right) = 1$ if $n \equiv 1(mod\ 4)$, and $\left(\frac{-1}{n}\right) = -1$ if $n \equiv -1(mod\ 4)$.
6. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$, i.e., $\left(\frac{2}{n}\right) = 1$ if $n \equiv \pm 1(mod\ 8)$, and $\left(\frac{2}{n}\right) = -1$ if $n \equiv \pm 3(mod\ 8)$.
7. For distinct odd positive coprime integers n and m,

$$\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}\left(\frac{n}{m}\right),$$

i.e., $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ if $n \equiv 1\,(mod\ 4)$ or $m \equiv 1\,(mod\ 4)$, and $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$ if $n \equiv -1\,(mod\ 4)$ and $m \equiv -1\,(mod\ 4)$ (*law of quadratic reciprocity*).

For example,

$$\left(\frac{-122}{45}\right) = \left(\frac{13}{45}\right) = \left(\frac{45}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right)$$
$$= (-1)\cdot\left(\frac{13}{3}\right) = (-1)\cdot\left(\frac{1}{3}\right) = (-1)\cdot 1 = -1.$$

It means that -122 is a quadratic nonresidue composite odd modulo 45.

For the proofs of the properties of Legendre symbol and Jacobi symbol as well as for some additional information, see, for example, [Buch09], [Gaus01], [DeKo13], and [IrRo90]. Historical aspects can be found in [Dick05], [Lege79], [Ore48], and [Wiki22].

Exercises

1. Check that $\left(\frac{-125}{47}\right) = 1$.
2. Find:

(a) $\left(\frac{102}{17}\right)$; (c) $\left(\frac{125}{47}\right)$; (e) $\left(\frac{-5000}{103}\right)$; (g) $\left(\frac{204}{311}\right)$;
(b) $\left(\frac{-88}{23}\right)$; (d) $\left(\frac{5000}{101}\right)$; (f) $\left(\frac{-1116}{73}\right)$; (h) $\left(\frac{219}{383}\right)$.

3. How many solutions has the congruence:

   (a) $x^2 - 200 \equiv 0(mod\ 79)$;
   (b) $x^2 \equiv 56(mod\ 87)$;
   (c) $x^2 \equiv 555(mod\ 101)$;
   (d) $x^2 \equiv 15(mod\ 209)$;
   (e) $x^2 + 27 \equiv 0(mod\ 91)$;
   (f) $x^2 \equiv 304(mod\ 299)$;
   (g) $x^2 - 990 \equiv 0(mod\ 1787)$;
   (h) $x^2 \equiv 500(mod\ 1777)$;
   (i) $x^2 - 270 \equiv (mod\ 2803)$?

4. Find the number of solutions to the congruence:

   (a) $2x^2 + 7x + 5 \equiv 0(mod\ 37)$;
   (b) $3x^2 + 5x + 7 \equiv 0(mod\ 87)$;
   (c) $2x^2 - 3x + 4 \equiv 0(mod\ 151)$;
   (d) $3x^2 - x + 7 \equiv 0(mod\ 151)$;
   (e) $5x^2 + 2x - 5 \equiv 0(mod\ 71)$;
   (f) $4x^2 - 2x + 9 \equiv 0(mod\ 137)$;
   (g) $5x^2 + 3x + 25 \equiv 0(mod\ 167)$;
   (h) $76x^2 - 77x + 36 \equiv 0(mod\ 227)$.

5. Find:

   (a) $\left(\frac{1001}{61}\right)$;
   (b) $\left(\frac{2741}{97}\right)$;
   (c) $\left(\frac{342}{667}\right)$;
   (d) $\left(\frac{342}{677}\right)$;
   (e) $\left(\frac{514}{327}\right)$;
   (f) $\left(\frac{514}{727}\right)$;
   (g) $\left(\frac{438}{593}\right)$;
   (h) $\left(\frac{232}{367}\right)$;
   (i) $\left(\frac{157}{379}\right)$;
   (j) $\left(\frac{438}{593}\right)$;
   (k) $\left(\frac{342}{677}\right)$;
   (l) $\left(\frac{2741}{97}\right)$;
   (m) $\left(\frac{1001}{61}\right)$;
   (n) $\left(\frac{514}{727}\right)$;
   (o) $\left(\frac{-88}{263}\right)$.

6. Find all primes p such that 3 is a quadratic nonresidue modulo p.
7. Find all prime divisors of the quadratic forms $2y^2+10$ and $3x^2+15$.

1.5. Multiplicative Orders, Primitive Roots, and Indexes

Multiplicative order

1.5.1. Given a positive integer n and an integer a coprime to n, the *multiplicative order* $ord_n\, a$ *of* a *modulo* n is defined as the smallest positive integer γ with

$$a^\gamma \equiv 1(mod\ n).$$

For example, $ord_5\, 4 = 2$, as $4^2 \equiv 1(mod\ 5)$, but $4^1 \not\equiv 1(mod\,5)$.

Similarly, $ord_5 3 = 4$, as $3^4 \equiv 1(mod\, 5)$, and $3^1 \not\equiv 1(mod\, 5)$, $3^2 \not\equiv 1(mod\, 5)$, and $3^3 \not\equiv 1(mod\, 5)$.

Finally, $ord_9 2 = 6$, as $2^6 \equiv 1(mod\, 9)$, and $2^1 \not\equiv 1(mod\, 9)$ and $2^2 \not\equiv 1(mod\, 9)$, $\ldots$, $2^5 \not\equiv 1(mod\, 9)$.

Properties of multiplicative order

1. If $a \equiv b(mod\ n)$, then $ord_n\, a = ord_n\, b$.
2. $ord_n\, a | \phi(n)$; in particular, $1 \leq ord_n\, a \leq \phi(n)$.
3. $a^\delta \equiv 1(mod\ n)$ if and only if $ord_n\, a | \delta$.
4. $a^\delta \equiv a^\eta (mod\ n)$ if and only if $\delta \equiv \eta(mod\ ord_n\, a)$.
5. The numbers $a^0, a^1, a^2, \ldots, a^{ord_n\, a - 1}$ represent different residue classes modulo n.
6. $ord_{p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}}\, a = lcm(ord_{p_1^{\alpha_1}}\, a, \ldots, ord_{p_s^{\alpha_s}}\, a)$.
7. $ord_m(a^n) = \frac{ord_m\, a}{gcd(n, ord_m\, a)}$.
8. If $ord_m\, a = \gamma_1 \cdot \gamma_2$, then $ord_m\, a^{\gamma_1} = \gamma_2$.
9. If $ord_{p^k}\, a = \gamma$, then $ord_{p^{k+1}}\, a \in \{\gamma, \gamma \cdot p\}$; if $ord_{p^k}\, a = \gamma$, $ord_{p^{k+1}}\, a = \gamma \cdot p$, and $p^k > 2$, then $ord_{p^{k+2}}\, a = \gamma \cdot p^2$.

For full proofs and examples, see [Buch09] and [DeKo13].

Primitive roots modulo n

1.5.2. If $ord_n\, g = \phi(n)$, g is called *primitive root* modulo n. In this case, the numbers

$$g^0, \ldots, g^{\phi(n)-1}$$

give all representatives of residue classes modulo n coprime to n.

For example, $\phi(5) = 4$. As $ord_5 3 = 4$, the number 3 is a primitive root modulo 5; as $ord_5 4 = 2$, the number 4 is not a primitive root modulo 5.

Similarly, $\phi(9) = 6$; as $ord_9 2 = 6$, the number 2 is a primitive root modulo 9; as $ord_9 7 = 3$ ($7^3 \equiv 1(mod\, 9)$, but $7^1 \not\equiv 1(mod\, 5)$ and $7^2 \not\equiv 1(mod\, 9)$), the number 7 is not a primitive root modulo 5.

Primitive roots exist only for $n = 2, 4, p^\alpha$, and $2p^\alpha$, where p is any odd prime number and α is any positive integer.

For full proofs and examples, see [Buch09], [DeKo13], and [Vino03].

Indexes

1.5.3. If g is a primitive root modulo n, then, for any a coprime with n, we have $a \equiv g^{\beta}(mod\ n)$, where $\beta \in [0, \phi(n) - 1]$. The number β is called *index* (or *discrete logarithm*) *of a modulo n with base g*. In this case, we write $\beta = ind\, a = ind_g\, a$.

For example, the number 3 is a primitive root modulo 5; in this case, the index of the number 4 modulo 5 with base 3 is 2, as $4 \equiv 3^2(mod\, 5)$. Moreover, as $3^0 \equiv 1(mod\, 5)$, $3^1 \equiv 3(mod\, 5)$, $3^2 \equiv 4(mod\, 5)$, and $3^3 \equiv 2(mod\, 5)$, we get $ind\, 1 = 0$, $ind\, 2 = 3$, $ind\, 3 = 1$, and $ind\, 4 = 2$.

Properties of indexes

1. If $a \equiv b(mod\ n)$, then $ind\, a \equiv ind\, b(mod\ \phi(n))$.
2. $ind\, a \cdot b \equiv ind\, a + ind\, b(mod\ \phi(n))$.
3. $ind\, a^k \equiv k \cdot ind\, a(mod\ \phi(n))$ for any non-negative integer k.
4. $ord_n\, a = \frac{\phi(n)}{gcd(ind\, a, \phi(n))}$.

Discrete logarithms are quickly computable in a few special cases. However, no efficient method is known for computing them in general. Several important algorithms in public-key cryptography base their security on the assumption that the discrete logarithm problem over carefully chosen groups has no efficient solution.

For the proofs of the properties of multiplicative orders, primitive roots and indexes, as well as some additional important information, see, for example, [Arno38], [BiBa70], [Buch09], [DeKo13], [DeKo18], [Dick05], [Gaus01], [Gelf98], [IrRo90], [Knut68], [Kost82], [Lege79], [Moze09], [Ore48], [Stra16], [Vino03], and [Wiki22].

Exercises

1. Find:

   (a) $ord_{35424}\, 17$;
   (b) $ord_{334368}\, (-17)$;
   (c) $ord_{6075}\, 8$;
   (d) $ord_{864}\, 625$;
   (e) $ord_{46575}\, 64$;
   (f) $ord_{48608}\, 125$;
   (g) $ord_{28768}\, 81$;
   (h) $ord_{203056}\, 125$;
   (i) $ord_{20000}\, 81$;
   (j) $ord_{99225}\, 16$;
   (k) $ord_{11^{50}}\, 5^{50}$;
   (l) $ord_{2^{2009}}\, 3$;
   (m) $ord_{2000}\, 343$;
   (n) $ord_{63072}\, 49$;
   (o) $ord_{253}\, 3^{55n+2}$.

2. Find all primitive roots modulo:

   (a) 12;
   (b) 14;
   (c) 50;
   (d) 81;
   (e) 98;
   (f) 242;
   (g) 250;
   (h) 338;
   (i) 625;
   (j) 1250.

3. Find all residue classes:

   (a) $[x]_{13}$, for which $ord_{13}\, x = 4$;
   (b) $[x]_{17}$, for which $ord_{17}\, x = 8$;
   (c) $[x]_{19}$, for which $ord_{19}\, x = 3$;
   (d) $[x]_{43}$, for which $ord_{43}\, x = 6$.

4. Find all indexes 11 modulo 5; modulo 7; and modulo 17.
5. Find the length of the period of the representation $\frac{a}{b} = 0,(q_1 \dots q_k \dots)_g$ if:

   (a) $\frac{a}{b} = \frac{221}{30000000},\ g = 7$;
   (b) $\frac{a}{b} = \frac{225}{70000},\ g = 4$;
   (c) $\frac{a}{b} = \frac{28}{99 \cdot 10^{12}},\ g = 3$;
   (d) $\frac{a}{b} = \frac{405}{242 \cdot 30^{10}},\ g = 8$.

6. Find $rest(37^{32^{90}}, 11)$ using properties of indexes.
7. How many solutions has the congruence:

   (a) $x^{12} \equiv 1 (mod\ 77)$;
   (b) $x^{12} \equiv 1 (mod\ 91)$;
   (c) $x^{12} \equiv 1 (mod\ 143)$;
   (d) $3x^{12} \equiv 31 (mod\ 41)$;
   (e) $x^{15} \equiv 1 (mod\ 451)$;
   (f) $x^{15} \equiv 1 (mod\ 287)$;
   (g) $x^{15} \equiv 1 (mod\ 143)$;
   (h) $x^{60} \equiv 79 (mod\ 97)$;
   (i) $x^{18} \equiv 1 (mod\ 77)$;
   (j) $x^{18} \equiv 1 (mod\ 91)$;
   (k) $x^{18} \equiv (mod\ 143)$;
   (l) $x^{55} \equiv 17 (mod\ 97)$?

8. Find:

   (a) $ord_{2^7 \cdot 11^5 \cdot 47}\, 7$;
   (b) $ord_{2^7 \cdot 13^3 \cdot 29}\, 11$;
   (c) $ord_{2^6 \cdot 7^3 \cdot 31}\, 3$;
   (d) $ord_{2^5 \cdot 11^3 \cdot 41^4}\, 3$;
   (e) $ord_{2^7 \cdot 13^3 \cdot 53}\, 7$;
   (f) $ord_{2^5 \cdot 3^3 \cdot 89}\, 125$;
   (g) $ord_{2^5 \cdot 3^3 \cdot 83}\, (-7)$;
   (h) $ord_{2^3 \cdot 3^2 \cdot 83}\, 49$.

1.6. Continued Fractions and Their Applications

Definition and simple properties

1.6.1. A *continued fraction* $[a_0, \ldots, a_n, \ldots]$ is defined as $a_0 + \frac{1}{a_1 + \frac{1}{\cdots \frac{1}{a_n + \cdots}}}$, where a_0 is some integer and all a_n, $n \in \mathbb{N}$, are positive integers (the last number, if it exists, $\neq 1$).

The rational numbers $\delta_k = [a_0, \ldots, a_k] = \frac{P_k}{Q_k}$, $k = 0, \ldots, n, \ldots$, are called *convergents* of the continued fraction $[a_0, \ldots, a_n, \ldots]$.

1.6.2. For example, consider a fraction $\frac{173}{281}$ and use for the numbers 173 and 281 the following Euclidean algorithm:

$$173 = 281 \cdot 0 + 173;\ 281 = 173 \cdot 1 + 108;\ 173 = 108 \cdot 1 + 65;$$

$$108 = 65 \cdot 1 + 43;\ 65 = 43 \cdot 1 + 22;\ 43 = 22 \cdot 1 + 21;$$

$$22 = 21 \cdot 1 + 1;\ 21 = 1 \cdot 21 + 0.$$

It is easy to see that

$$\frac{173}{281} = 0 + \frac{1}{\frac{281}{173}},\ \frac{281}{173} = 1 + \frac{1}{\frac{173}{108}}, \ldots,$$

$$\frac{65}{22} = 1 + \frac{1}{\frac{43}{21}},\ \frac{43}{21} = 1 + \frac{1}{\frac{22}{21}}, \frac{22}{21} = 1 + \frac{1}{21}.$$

Therefore,

$$\frac{173}{281} = 0 + \frac{1}{1 + \frac{1}{\cdots + \frac{1}{21}}} = [0, 1, 1, 1, 1, 1, 1, 21].$$

The convergents of the continued fraction $[0, 1, 1, 1, 1, 1, 1, 21]$ are: $\delta_0 = [0] = 0$; $\delta_1 = [0, 1] = 0 + \frac{1}{1} = 1$; $\delta_2 = [0, 1, 1] = 0 + \frac{1}{1 + \frac{1}{1}} = 0 + \frac{1}{2} = \frac{1}{2}$; $\delta_3 = [0, 1, 1, 1] = \frac{2}{3}$; $\delta_4 = [0, 1, 1, 1, 1] = \frac{3}{5}$; $\delta_5 = [0, 1, 1, 1, 1, 1] = \frac{5}{8}$; $\delta_6 = [0, 1, 1, 1, 1, 1, 1] = \frac{8}{13}$; and $\delta_7 = [0, 1, 1, 1, 1, 1, 1, 21] = \frac{173}{281}$.

For the decomposition of $\frac{1 - 3\sqrt{5}}{2}$, we use a generalization of the Euclidean algorithm.

As $6 < \sqrt{45} < 7$, we obtain for $\frac{1 - 3\sqrt{5}}{2} = \frac{1 - \sqrt{45}}{2}$ the following estimation: $-3 < \frac{1 - 3\sqrt{5}}{2} < -2.5$, i.e., $a_0 = \lfloor \frac{1 - 3\sqrt{5}}{2} \rfloor = -3$. Then, $\alpha_0 = \frac{1 - 3\sqrt{5}}{2} = -3 + \frac{1}{\alpha_1}$, where $\frac{1}{\alpha_1} = \frac{1 - 3\sqrt{5}}{2} - (-3) = \frac{7 - 3\sqrt{5}}{2}$.

Therefore, $\alpha_1 = \frac{2}{7-3\sqrt{5}} = \frac{2(7+3\sqrt{5})}{(7-3\sqrt{5})(7+3\sqrt{5})} = \frac{2(7+3\sqrt{5})}{49-45} = \frac{2(7+3\sqrt{5})}{4} = \frac{(7+3\sqrt{5})}{2}$.

As $6.5 < \frac{(7+3\sqrt{5})}{2} < 7$, we get $a_1 = \lfloor\frac{(7+3\sqrt{5})}{2}\rfloor = 6$ and $\alpha_1 = \frac{7+3\sqrt{5}}{2} = 6 + \frac{1}{\alpha_2}$, where $\frac{1}{\alpha_2} = \frac{7+3\sqrt{5}}{2} - 6 = \frac{-5+3\sqrt{5}}{2}$.

Therefore, $\alpha_2 = \frac{2}{-5+3\sqrt{5}} = \frac{2(-5-3\sqrt{5})}{(-5+3\sqrt{5})(-5-3\sqrt{5})} = \frac{2(-5-3\sqrt{5})}{25-45} = \frac{2(5+3\sqrt{5})}{20} = \frac{(5+3\sqrt{5})}{10}$.

As $1.1 < \frac{(5+3\sqrt{5})}{10} < 1.2$, then $a_2 = \lfloor\frac{(5+3\sqrt{5})}{10}\rfloor = 1$ and $\alpha_2 = \frac{5+3\sqrt{5}}{10} = 1 + \frac{1}{\alpha_3}$, where $\frac{1}{\alpha_3} = \frac{5+3\sqrt{5}}{10} - 1 = \frac{-5+3\sqrt{5}}{10}$.

Therefore, $\alpha_3 = \frac{10}{-5+3\sqrt{5}} = \frac{10(-5-3\sqrt{5})}{(-5+3\sqrt{5})(-5-3\sqrt{5})} = \frac{10(-5-3\sqrt{5})}{25-45} = \frac{10(5+3\sqrt{5})}{20} = \frac{(5+3\sqrt{5})}{2}$.

As $5.5 < \frac{(5+3\sqrt{5})}{2} < 6$, then $a_3 = \lfloor\frac{(5+3\sqrt{5})}{2}\rfloor = 5$ and $\alpha_3 = \frac{5+3\sqrt{5}}{2} = 5 + \frac{1}{\alpha_4}$, where $\frac{1}{\alpha_4} = \frac{5+3\sqrt{5}}{2} - 5 = \frac{-5+3\sqrt{5}}{2}$.

So, $\frac{1}{\alpha_4} = \frac{1}{\alpha_2}$, i.e., $\alpha_4 = \alpha_2$. Therefore, $\alpha_4 = \frac{5+3\sqrt{5}}{10} = 1 + \frac{1}{\alpha_5}$, where $\frac{1}{\alpha_5} = \frac{-5+3\sqrt{5}}{10}$. In particular, $a_4 = a_2$, and $\frac{1}{\alpha_5} = \frac{1}{\alpha_3}$, i.e., $\alpha_5 = \alpha_3$. Similarly, $a_5 = a_3$ and $\frac{1}{\alpha_6} = \frac{1}{\alpha_4}$, i.e., $\alpha_6 = \alpha_4$; in the same way, $a_6 = a_4$ and $\frac{1}{\alpha_7} = \frac{1}{\alpha_5}$, i.e., $\alpha_7 = \alpha_5$, etc.

So, we get the decomposition

$$\begin{aligned}\frac{1-3\sqrt{5}}{2} &= [a_0, a_1, a_2, a_3, a_4, \ldots] = [-3, 6, 1, 5, 1, 5, 1, 5, \ldots] \\ &= [-3, 6, (1, 5)].\end{aligned}$$

The convergents of the continued fraction $[-3, 6, 1, 5, 1, 5, 1, 5, \ldots]$ are: $\delta_0 = [-3] = -3$; $\delta_1 = [-3, 6] = -3 + \frac{1}{6} = -\frac{17}{6}$; $\delta_2 = [-3, 6, 1] = -3 + \frac{1}{6+\frac{1}{1}} = -3 + \frac{1}{7} = -\frac{20}{7}$, $\delta_3 = [-3, 6, 1, 5] = -\frac{117}{41}$, $\delta_4 = [-3, 6, 1, 5, 1] = -\frac{137}{48}$, etc.

1.6.3. Continued fractions are motivated by a desire to have a "mathematically pure" representation for the real numbers.

Properties of continued fractions

1. If $\delta_k = \frac{P_k}{Q_k}$, then $P_0 = a_0$, $P_1 = a_1a_0 + 1$, and $P_n = a_nP_{n-1} + P_{n-2}$ for any $n \geq 2$.

2. If $\delta_k = \frac{P_k}{Q_k}$, then $Q_0 = 1$, $Q_1 = a_1$, and $Q_n = a_nQ_{n-1} + Q_{n-2}$ for any $n \geq 2$.
3. $gcd(P_n, Q_n) = 1$.
4. $1 = Q_0 \leq Q_1 < Q_2 < \cdots$.
5. If $P_0 > 1$, then $P_1 > P_2 > P_3 > \cdots$.
6. $\delta_n - \delta_{n-1} = \frac{(-1)^{n+1}}{Q_nQ_{n-1}}$.
7. $\delta_0 < \delta_2 < \cdots < \delta_3 < \delta_1$.
8. Every finite continued fraction is rational, and every rational number can be represented in precisely one way as a finite continued fraction.
9. Every infinite continued fraction is irrational, and every irrational number can be represented in precisely one way as an infinite continued fraction.
10. A continued fraction is periodic if and only if it is the continued fraction representation of a quadratic irrational, that is, a real solution to a quadratic equation with integer coefficients.
11. $[a_0, \ldots, a_n, \ldots] = \frac{\alpha_nP_{n-1}+P_{n-2}}{\alpha_nQ_{n-1}+Q_{n-2}}$, where $\alpha_n = [a_n, \ldots]$.
12. If $\alpha = [a_0, \ldots, a_n, \ldots]$, then $|\alpha - \delta_n| \leq \frac{1}{Q_nQ_{n+1}}$; in particular, for any $n > 1$, δ_n is the best rational approximation for α.

Applications of continued fractions

Continued fractions have some important applications.

1.6.4. They can be used for rational approximations of a given real number. Moreover, using continued fractions, one can obtain the so-called *best rational approximations.*

In fact, we define a *best rational approximation* to a real number α as a rational number $\frac{a}{b}$, $b > 0$, that is closer to α than any approximation with a smaller or equal denominator. In other words, if $\frac{a}{b}$ is a best approximation to α, then the condition $|\alpha - \frac{x}{y}| < |\alpha - \frac{a}{b}|$ holds only for rational numbers $\frac{x}{y}$ with $y > b$.

The continued fraction $\alpha = [a_0, a_1, \ldots, a_n, \ldots]$ for α can be used to generate all of the best rational approximations for α. In fact, *any convergent* $\delta_k = [a_0, a_1, \ldots, a_k]$, $k = 1,2,\ldots$, *is a best rational approximation to* α.

In order to get a best approximation with a given accuracy Δ, we consider the denominators Q_0, Q_1, $\ldots$, Q_n, Q_{n+1}, $\ldots$ of convergents $\delta_0, \delta_1, \ldots . \delta_n, \delta_{n+1}, \ldots$ of decomposition $\alpha = [a_0, a_1, \ldots, a_n, a_{n+1}, \ldots]$. If $Q_n Q_{n+1} \geq \Delta^{-1}$, we use as the best approximation with a given accuracy Δ the nth convergent δ_n: $\alpha \approx \delta_n$: as $|\alpha - \delta_n| \leq |\delta_{n+1} - \delta_n| = \frac{1}{Q_{n+1}Q_n}$ and $Q_n Q_{n+1} \geq \Delta^{-1}$, then

$$|\alpha - \delta_n| \leq \Delta.$$

For example, if we are going to find the best approximation of $-\sqrt{15}$ with the accuracy $\Delta = 10^{-3}$, we should find the decomposition of $-\sqrt{15}$ into a continued fraction:

$\alpha_0 = -\sqrt{15} = -4 + \frac{1}{\alpha_1}$, where $\frac{1}{\alpha_1} = 4 - \sqrt{15}$;

$\alpha_1 = 4 + \sqrt{15} = 7 + \frac{1}{\alpha_2}$, where $\frac{1}{\alpha_2} = -\mathbf{3} + \sqrt{\mathbf{15}}$;

$\alpha_2 = \frac{3+\sqrt{15}}{6} = 1 + \frac{1}{\alpha_3}$, where $\frac{1}{\alpha_3} = \frac{-3+\sqrt{15}}{6}$;

$\alpha_3 = 3 + \sqrt{15} = 6 + \frac{1}{\alpha_4}$, where $\frac{1}{\alpha_4} = -\mathbf{3} + \sqrt{\mathbf{15}}$.

So, $-\sqrt{15} = [-4, 7, (1, 6)]$.

Find the smallest index n such that $Q_{n+1} \cdot Q_n \geq \frac{1}{\Delta} = 10^3$.

n	-2	-1	0	1	2	3	4
a_n			-4	7	1	6	1
P_n	0	1					
Q_n	1	0	1	7	8	55	63

As $1 \cdot 7 < 10^3$, $7 \cdot 8 < 10^3$, and $8 \cdot 55 < 10^3$, while $55 \cdot 63 > 10^3$, we should stop at $Q_4 = 63$ (see the table above). So, $n = 3$, and we choose as the best approximation to $-\sqrt{15}$ the third convergent $\delta_3 = \frac{P_3}{Q_3}$. For calculating P_3, use the following table.

n	-2	-1	0	1	2	3	4
a_n			-4	7	1	6	1
P_n	0	1	-4	-27	-31	-213	-234
Q_n	1	0	1	7	8	55	63

Therefore, $\alpha \approx -\frac{213}{55}$ with accuracy 10^{-3}.

1.6.5. Continued fractions play an essential role in solving some Diophantine equations.

The simplest Diophantine equation, e.g., a *linear Diophantine equation*, takes the form

$$ax + by = c.$$

This Diophantine equation has a solution (where x and y are integers) if and only if c is a multiple of the greatest common divisor of a and b: $gcd(a, b)|c$. Moreover, if (x_0, y_0) is a solution, then the other solutions have the form $x = x_0 \pm \frac{b}{gcd(a,b)}t$, $y = y_0 \mp \frac{a}{gcd(a,b)}t$, where t is an arbitrary integer.

Without loss of generality, let $gcd(a, b) = 1$ (otherwise divide all three coefficients a, b, and c of the equation $ax+by = c$ by the number $gcd(a, b)$). In this case, decompose the rational number $\frac{a}{b}$ into a finite continued fraction $[a_0, a_1, \ldots, a_n]$. As $P_sQ_{s-1} - Q_sP_{s-1} = (-1)^{s-1}$, then for $s = n$, we get the equality $P_nQ_{n-1} - Q_nP_{n-1} = (-1)^{n-1}$. As $\frac{a}{b} = \frac{P_n}{Q_n}$ and $gcd(a, b) = 1$, then $a = P_n$ and $b = Q_n$, i.e., $aQ_{n-1} - bP_{n-1} = (-1)^{n-1}$. Using a multiple $(-1)^{n-1}c$, we get

$$a((-1)^{n-1}c \cdot Q_{n-1}) + b((-1)^n c \cdot P_{n-1}) = c,$$

i.e., find a solution $(x_0, y_0) = ((-1)^{n-1}c \cdot Q_{n-1}, (-1)^n c \cdot P_{n-1})$ of the equation $ax + by = c$. Therefore, all solutions of the equation $ax + by = c$ can be now expressed as $x = x_0 \pm bt$, $y = y_0 \mp at$, where $t \in \mathbb{Z}$.

For example, consider the equation $33x + 51y = 21$.

It is equivalent to the equation $11x + 17y = 7$, where $gcd(11, 17) = 1$. Get the decomposition of the number $\frac{17}{11}$ into a finite continued fraction:

$17 = 11 \cdot 1 + 6;$
$11 = 6 \cdot 1 + 5;$
$6 = 5 \cdot 1 + 1;$
$5 = 1 \cdot 5 + 0.$

So, $\frac{17}{11} = [1, 1, 1, 5]$.

Find the convergents of $[1, 1, 1, 5]$ using the following table.

n	-2	-1	0	1	2	3
a_n			1	1	1	5
P_n	0	1	1	2	3	17
Q_n	1	0	1	1	2	11

As $P_sQ_{s-1} - Q_sP_{s-1} = (-1)^{s-1}$, then for $s = 3$, we get that $17 \cdot 2 - 11 \cdot 3 = 1$, or $11 \cdot (-3) + 17 \cdot 2 = 1$. Hence, $11 \cdot (-21) + 17 \cdot 14 = 7$. Therefore, we get a solution (x_0, y_0) of the equation $11x + 17y = 7$ in the form $(-21, 14)$. In this case, all the solutions to the equation $11x + 17y = 7$ can be obtained as $x = -21 + 17t, y = 14 - 11t$, where $t \in \mathbb{Z}$.

1.6.6. Continued fractions are used in solving the *Pell's equation*, $x^2 - Dy^2 = \pm 1$, where D is a positive integer, which is not a perfect square.

In fact, if $\sqrt{D}$ has the continued fraction's decomposition $\sqrt{D} = [a_0, (a_1, a_1, \dots, a_{k-1}, 2a_0)]$ with period k, then all positive integer solutions of the Pell's equation $x^2 - Dy^2 = 1$ have the form $x = P_{kn-1}$, $y = Q_{kn-1}$, where $n \in \mathbb{N}$ and kn is even. So, the equation $x^2 - Dy^2 = 1$ has infinitely many solutions [Buch09].

Similarly, all positive integer solutions of the Pell's equation $x^2 - Dy^2 = -1$ can be found by the formulas $x = P_{kn-1}$, $y = Q_{kn-1}$, where $n \in \mathbb{N}$ and kn is odd. So, the equation $x^2 - Dy^2 = -1$ has infinitely many solutions for odd k and no solutions for even k [Buch09].

For example, try to find the first four solutions of the equations $x^2 - 3y^2 = 1$ and $x^2 - 3y^2 = -1$.

For that, find the decomposition of the number $\sqrt{3}$ into a continued fraction:

$\alpha_0 = \sqrt{3} = 1 + \frac{1}{\alpha_1}$, where $\frac{1}{\alpha_1} = \mathbf{-1 + \sqrt{3}}$;
$\alpha_1 = \frac{1+\sqrt{3}}{2} = 1 + \frac{1}{\alpha_2}$, where $\frac{1}{\alpha_2} = \frac{-1+\sqrt{3}}{2}$;
$\alpha_2 = 1 + \sqrt{3} = 2 + \frac{1}{\alpha_3}$, where $\frac{1}{\alpha_3} = \mathbf{-1 + \sqrt{3}}$.

So, $\sqrt{3} = [1, (1, 2)]$, i.e., the length k of the period of decomposition of $\sqrt{3}$ is 2.

Therefore, all positive integer solutions of the equation $x^2-3y^2 = 1$ can be found as $x = P_{2n-1}$, $y = Q_{2n-1}$, where $n \in \mathbb{N}$. The first four solutions (P_1, Q_1), (P_3, Q_3), (P_5, Q_5), and (P_7, Q_7) are obtained for $n = 1, 2, 3$, and 4.

Find these solutions using the following table.

n	-2	-1	0	1	2	3	4	5	6	7
a_n			1	1	2	1	2	1	2	1
P_n	0	1	1	2	5	7	19	26	71	97
Q_n	1	0	1	1	3	4	11	15	41	56

So, the first four solutions of the equation $x^2 - 3y^2 = 1$ are $(P_1, Q_1) = (2, 1)$, $(P_3, Q_3) = (7, 4)$, $(P_5, Q_5) = (26, 15)$, and $(P_7, Q_7) = (97, 56)$.

All positive integer solutions of the equation $x^2-Dy^2 = -1$ should have the form $x = P_{kn-1}$, $y = Q_{kn-1}$, where $n \in \mathbb{N}$ and kn is odd. In our case $(k = 2)$, it is impossible, and the equation $x^2 - 3y^2 = -1$ has no solutions.

1.6.7. In algebraic constructive methods of computations of amicable numbers, we often should consider bilinear Diophantine equations of the form

$$axy - b(x + y) = c, \; gcd(a, b, c) = 1.$$

(See, for example, [Yan96].)

Solutions of such equations can be found by using the continued fraction method above and after solving a quadratic equation to get x and y.

But in this case, the most systematic method to solve the equation $axy-b(x+y) = c$, $gcd(a, b, c) = 1$ is the integer factorization method via some combinatorial computations. It is easy to see that in this case, we get the equation

$$(ax - b)(ay - b) = w, \; w = ac + b^2.$$

Factoring w and writing it as a product $w = uv$, we get $u = ax - b$, $v = ay - b$, and hence, $x = \frac{u+b}{a}$, $y = \frac{v+b}{a}$. Usually, w can be written as $w = uv$ in many ways, and there is a good chance to get new amicable pairs [Yan96].

For the proof of the properties of continued fractions and for some additional information, see, for example, [Buch09], [Dave99], [DeKo13], and [Khin97]. The historical aspect of the question can be found in [Dick05] and [Ore48]. Some number-theoretical applications are provided by [DeDe12].

Exercises

1. Find the decomposition into a continuous fraction:
   - (a) $\frac{312}{175}$;
   - (b) $-\frac{19}{15}$;
   - (c) $\frac{72}{103}$;
   - (d) $\frac{3885}{2306}$;
   - (e) $-\frac{1000}{3333}$;
   - (f) $\frac{27899}{36823}$.
2. Find the decomposition into a continuous fraction:
   - (a) $\frac{1+3\sqrt{2}}{2}$;
   - (b) $\frac{1-3\sqrt{2}}{2}$;
   - (c) $\frac{1+3\sqrt{5}}{2}$;
   - (d) $\frac{1-3\sqrt{5}}{2}$;
   - (e) $\frac{1+2\sqrt{6}}{5}$;
   - (f) $\frac{1+3\sqrt{3}}{2}$;
   - (g) $\frac{2-2\sqrt{6}}{5}$;
   - (h) $\frac{2+2\sqrt{6}}{5}$;
   - (i) $\frac{6+2\sqrt{2}}{7}$;
   - (j) $\frac{6-5\sqrt{2}}{7}$;
   - (k) $\frac{-15-6\sqrt{2}}{8}$;
   - (l) $\frac{6\sqrt{2}-15}{8}$.
3. Find the decomposition into a continuous fraction:
   - (a) $\frac{\sqrt{2210}-13}{13}$;
   - (b) $\frac{169+\sqrt{63005}}{158}$;
   - (c) $\frac{1170+2\sqrt{93637}}{232}$.
4. Find the rational number represented as:
   - (a) $[1, 2, 3, 4, 6]$;
   - (b) $[-2, 111, 2, 1, 3]$;
   - (c) $[-2, 3, 3, 10]$;
   - (d) $[-1, 2, 3, 10]$;
   - (e) $[-2, 1, 3, 7]$;
   - (f) $[-3, 1, 3, 9, 5]$;
   - (g) $[1, 2, 3, 4, 6]$;
   - (h) $[0, 8, 1, 6, 2, 2]$.
5. Find the irrational number represented as:
   - (a) $[1, (2)]$;
   - (b) $[2, (4)]$;
   - (c) $[3, (6)]$;
   - (d) $[4, (8)]$;
   - (e) $[5, (10)]$;
   - (f) $[6, (12)]$;
   - (g) $[7, (14)]$;
   - (h) $[8, (16)]$;
   - (i) $[2, (1, 4)]$;
   - (j) $[2, (2, 4)]$;
   - (k) $[3, (1, 6)]$;
   - (l) $[3, (2, 6)]$;
   - (m) $[3, (3, 6)]$;
   - (n) $[4, (1, 8)]$;
   - (o) $[4, (2, 8)]$;
   - (p) $[3, (10, 5)]$;
   - (q) $[3, (1, 5)]$;
   - (r) $[3, (4, 1)]$;
   - (s) $[5, (2, 10)]$;
   - (t) $[-3, 6, (1, 5)]$.

6. Find a rational approximation of $\sqrt{10}$ with accuracy $\Delta = 5 \cdot 10^{-3}$.
7. Find a rational approximation of $\sqrt{21}$ with accuracy $\Delta = 0^{-4}$.
8. Find the best approximation of $\frac{2500}{1441}$ $\left(\frac{1292}{479}\right)$ by the fraction $\frac{a}{b}$ with $b \leq 100$. Find the accuracy of his approximation.
9. Solve the equation:

   (a) $311x + 28y = 2$;
   (b) $26x + 91y = 11$;
   (c) $253x - 449y = 3$;
   (d) $73x + 85y = 7$.

10. Find the first four positive integer solutions of the equation:

   (a) $x^2 - 5y^2 = 1$;
   (b) $x^2 - 5y^2 = -1$;
   (c) $x^2 - 19y^2 = 1$;
   (d) $x^2 - 19y^2 = -1$.

11. Find the smallest positive integer solution to the equation:

   (a) $x^2 - 41y^2 = 1$;
   (b) $x^2 - 41y^2 = -1$;
   (c) $x^2 - 13y^2 = -1$;
   (d) $x^2 - 13y^2 = -1$.

References

[IrRo90], [Arno38], [BiBa70], [BaCo87], [Buch09], [CoRo96], [Dave99], [Dede63], [DeKo13], [Gelf98], [HaWr79], [Lagr70], [Lege79], [LiNi96], [LiNi96], [MSC96], [Moze09], [Nage51], [Ore48], [RaTo57], [Smit84], [Hons91], [Plut78], [Stra16], [Stru87], [Vino03].

Chapter 2

Arithmetic Functions

2.1. Additive and Multiplicative Functions

2.1.1. A complex-valued function $f(n)$ is called an *arithmetic function* (or *arithmetical function* or *number-theoretic function*) if the value $f(n)$ is determined for any positive integer n.

Some authors include in this definition the requirement that an arithmetic function "expresses some arithmetical properties of n."

Over the last 400 years, number theorists have studied dozens of different arithmetic functions. Prominent examples include the divisor function, the Euler's totient function, the Möbius function, the Liouville function, Dirichlet characters, the prime counting function, the von Mangoldt function, and partition functions.

Arithmetic functions describe number-theoretical (arithmetic) properties of numbers and are widely used in the field of number theory.

Arithmetic functions are different from typical functions in that they cannot usually be described by simple formulas, so they are often evaluated in terms of their average or asymptotic behavior.

This is partially motivated by historical connections with the prime number theorem as well as proving theoretical guarantees for cryptographic applications, which usually rely on very large numbers to provide security. The two main methods of analyzing arithmetic functions are asymptotic analysis and average order analysis.

Arithmetic functions have applications in combinatorics, counting, and probability theory and analysis, in which they arise as coefficients of power series.

2.1.2. Most of the important arithmetic functions exhibit convenient behavior under addition or multiplication. This is not too surprising since arithmetic functions describe properties of positive integers which are closed under addition and multiplication. Arithmetic functions that exhibit these properties under addition are known as *additive functions*, while those under multiplication are known as *multiplicative functions.*

An *additive function* is an arithmetic function $f(n)$ of the positive integer n with the property that the function of a product of coprime positive integers m and n is the sum of the functions on those integers:

$$f(mn) = f(m) + f(n) \quad \text{if } gcd(m,n) = 1.$$

An arithmetic function $f(n)$ is said to be completely (totally) additive if $f(mn) = f(m) + f(n)$ holds for all positive integers m and n, even when they are not coprime.

An arithmetic function f is called *multiplicative* if $f(1) = 1$, and the function of a product of coprime positive integers m and n is the product of the functions on those integers:

$$f(m \cdot n) = f(m) \cdot f(n) \quad \text{if } gcd(m,n) = 1.$$

A multiplicative function f is called *completely multiplicative* if the condition $f(m \cdot n) = f(m) \cdot f(n)$ holds for any positive integers m and n.

For example, the function $f(n) = n^{\alpha}$ is completely multiplicative for any real number α. The divisor function, the Möbius function, and the Euler's toient function are multiplicative but not completely multiplicative. The prime counting function $\pi(x)$ is not a multiplicative function.

2.1.3. Examples of additive and multiplicative functions include many functions of importance in number theory, such as:

- $\nu(n)$: the number of distinct primes dividing n; additive function;
- the sum of the distinct primes dividing n; additive function;
- $\Omega(n)$: the total number of prime factors of n, counting multiple factors multiple times (the *big omega function*); completely additive function;
- the *multiplicity of a prime factor* p in n, that is the largest exponent m for which p^m divides n; completely additive function;
- the sum of primes dividing n counting multiplicity (the *potency* of n or the *integer logarithm* of n); completely additive function;
- $\phi(n)$: the Euler's totient function, counting the positive integers coprime to (but not bigger than) n; multiplicative function;
- $\mu(n)$: the Möbius function related to the number of prime factors of square-free numbers; multiplicative function;
- $gcd(n, k)$: the greatest common divisor of n and k, where k is a fixed integer; multiplicative function;
- $\tau(n)$: the number of positive divisors of n; multiplicative function;
- $\sigma(n)$: the sum of positive divisors of n; multiplicative function;
- $\sigma_x(n)$: the sum of the xth powers of all the positive divisors of n (where x may be any complex number); in special cases, we have $\sigma_0(n) = \tau(n)$ and $\sigma_1(n) = \sigma(n)$; multiplicative function;
- $1(n)$: the constant function, defined by $1(n) = 1$ for any positive integer n; completely multiplicative function;
- $1_C(n)$: the indicator function of the set C, containing 1 (of squares, or cubes, or fourth powers, etc.); $1_C(n) = 1$, if $n \in C$, and $1_C(n) = 0$ otherwise; completely multiplicative function;
- $Id(n)$: identity function, defined by $Id(n) = n$ for any positive integer n; completely multiplicative function;
- $Id_x(n)$, $x \in \mathbb{C}$: the power function, defined by $Id_x(n) = n^x$ for any positive integer n; as special cases, we have $Id_0(n) = 1(n)$ and $Id_1(n) = Id(n)$; completely multiplicative function;
- $\epsilon(n)$: the function defined by $\epsilon(n) = 1$ if $n = 1$, and $\epsilon(n) = 0$ if $n > 1$, sometimes called *multiplication unit for Dirichlet convolution* (or simply the *unit function*); completely multiplicative function;
- $\left(\frac{n}{p}\right)$: the *Legendre symbol*, where p is a fixed odd prime number; completely multiplicative function;

- $\lambda(n)$: the Liouville function, defined as $\lambda(n) = (-1)^{\Omega(n)}$, where $\Omega(n)$ is the number of prime factors of n, counted with multiplicity; completely multiplicative function;
- $\gamma(n)$: the function, defined by $\gamma(n) = (-1)^{\nu(n)}$, where the additive function $\nu(n)$ is the number of distinct primes dividing n; completely multiplicative function;
- Dirichlet character modulo m; completely multiplicative function.

Examples of a non-additive and a non-multiplicative function are given by the *prime counting function* $\pi(x) = \sum_{p \leq x, p \in P}$, giving the number of primes less than or equal to given positive real x; by the *Mangoldt function* $\Lambda(n)$, equal to $\log p$ for $n = p^\alpha$ $p \in P, \alpha \in \mathbb{N}$, and equal to 0 otherwise; by *restricted divisor function* $s(n) = \sum_{d|n,\ d \neq n} d$, $n \in \mathbb{N}$; etc.

For example, consider an arithmetic function $r_2(n)$, giving the number of representations of n as a sum of squares of two integers, positive, negative, or zero, where in counting the number of ways, reversal of order is allowed. As $1 = 1^2 + 0^2 = (-1)^2 + 0^2 = 0^2 + 1^2 = 0^2 + (-1)^2$, then $r_2(1) = 4 \neq 1$. This shows that the function is not multiplicative. However, $\frac{r_2(n)}{4}$ is multiplicative.

2.1.4. In the following, we list several well-known properties of additive and multiplicative functions, which are important for our further consideration.

Properties of multiplicative functions

1. If f and g are multiplicative functions, then $f \cdot g$ is a multiplicative function.
2. If f is a multiplicative function, then for a given $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$, it holds that

$$\sum_{d|n} f(d) = \prod_{i=1}^{s} (1 + f(p_i) + f(p_1^2) + \cdots + f(p_s^{\alpha_s})).$$

3. If f is a multiplicative function, then $h(n) = \sum_{d|n} f(d)$ is a multiplicative function.

4. If f and g are two multiplicative functions, then the *Dirichlet convolution* $f * g$ of f and g, defined by $(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$, is a multiplicative function.
5. A multiplicative function f is completely determined by its values at the powers of prime numbers: $f(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = f(p_1^{\alpha_1}) \cdot f(p_2^{\alpha_2}) \cdot \ldots \cdot f(p_s^{\alpha_s})$.
6. A completely multiplicative function f is completely determined by its values at the prime numbers: $f(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = f(p_1)^{\alpha_1} \cdot f(p_2)^{\alpha_2} \cdot \ldots \cdot f(p_s)^{\alpha_s}$.
7. An additive function f is completely determined by its values at the powers of prime numbers: $f(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = f(p_1^{\alpha_1}) + f(p_2^{\alpha_2}) + \cdots + f(p_s^{\alpha_s})$.
8. A completely additive function f is completely determined by its values at the prime numbers: $f(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = f(p_1)^{\alpha_1} + f(p_2)^{\alpha_2} + \cdots + f(p_s)^{\alpha_s}$.
9. If f is a multiplicative function and a, b are any two positive integers, then $f(a) \cdot f(b) = f(gcd(a, b)) \cdot f(lcm(a, b))$.
10. If $f(n)$ is a (completely) additive function, then $g(n) = (-1)^{f(n)}$ is a (completely) multiplicative function.

□ Consider, for example, the proof of the third property. If m and m are coprime, then for any divisor d of mn, one can write it as $d = d_1d_2$, where d_1 and d_2 are coprime and $d_1|m$, $d_2|m$. Then, we have that

$$\begin{aligned} h(mn) &= \sum_{d|mn} f(d) = \sum_{d_1|m, d_2|n} f(d_1d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) = h(m)h(n). \end{aligned}$$

Moreover, prove property 4 for the Dirichlet convolution $h(n) = f * g(n)$. Let $gcd(m, n) = 1$. If $d|mn$ and since $(m, n) = 1$, there exist unique integers a, b such that $a|m$, $b|n$, and $d = ab$. Therefore,

$$h(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = \sum_{a|m} \sum_{b|n} f(ab)g\left(\frac{mn}{ab}\right).$$

Since $gcd(m,n) = 1$, then $(a,b) = 1$. Furthermore, $gcd(\frac{m}{a}, \frac{n}{b}) = 1$. Since f and g are multiplicative, we have that

$$\begin{aligned} h(mn) &= \sum_{a|m} \sum_{b|n} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) \\ &= \left(\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right) \cdot \left(\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right) = h(m)h(n). \end{aligned}$$

Therefore, h is multiplicative.

With the operation of the Dirichlet convolution $f * g$, the set of all multiplicative functions turns into an abelian group; the identity element is ϵ. □

2.1.5. The additive and multiplicative properties of certain arithmetic functions greatly simplify their analysis since they are determined only by their values at primes and prime powers. The average and asymptotic behavior of prime numbers has been well studied, so additive and multiplicative functions are more easily analyzed than non-additive and non-multiplicative arithmetic functions.

In addition, many series of the natural numbers can be simplified when factored into a product over the primes. One example is the Euler product, which expresses a Dirichlet series as an infinite product over the primes, assuming the series terms have certain multiplicative properties. The Euler product is historically important as it was introduced by Leonhard Euler in his proof of the connection between the Riemann zeta function and the prime numbers (see Section 2.5 of this chapter).

Furthermore, the values of additive or multiplicative functions can be efficiently calculated in computational number theory using memorization for arguments which are smooth numbers. This is especially useful for functions which might otherwise take linear time in naive implementations, such as Euler's totient function.

The computational convenience of such functions is central to the development of modern cryptographic methods. Specifically, many cryptographic applications rely on using very large numbers (often in the hundreds of digits) to encode information, and their security often depends on the difficulty of inverting the value of certain arithmetic functions. These functions are often chosen to be multiplicative since this allows fast and memory-efficient computation on very large values, crucial to applications such as network encryption. However, because these functions are easy to compute given the prime factorization of a number, they are also relatively easy to invert given the prime factorization. Luckily, determining the prime factorization of a large number is difficult, so cryptographic methods can utilize the strengths of multiplicative functions without succumbing to their weaknesses.

In this chapter, we consider history, main properties, and most important applications of some classical arithmetic functions. The main goal is to study the divisor function and its relatives, as this function plays an important role in the definition and investigation of all classes of special numbers under our consideration.

For additional information, see, for example, [DeKo18], [Dick05], [Ore48], [Salo90], [Sier64], [Prim22], and [Wiki22].

Exercises

1. Prove that the function $f(n) = n^2$ is completely multiplicative; what can be said about the function $g(n) = \log f(n)$?
2. For $n = 1, 2, 3, \ldots, 20, 100, 2000$, find $\nu(n)$, the number of distinct primes dividing n; prove that $\nu(n)$ is an additive function; is it completely additive? What can be said about the function $\gamma(n) = (-1)^{\nu(n)}$?
3. For $n = 1, 2, 3, \ldots, 20, 1000, 2000$, find the sum of the distinct primes dividing n; prove that it is an additive function; is it completely additive?
4. For $n = 1, 2, 3, \ldots, 20, 100, 2000$, find $\Omega(n)$, the total number of prime factors of n, counting multiple factors multiple times; prove that $\Omega(n)$ is an additive function; is it completely additive? What can be said about the Liouville function, defined as $\lambda(n) = (-1)^{\Omega(n)}$?
5. For $n = 1, 2, 3, \ldots, 20, 100, 2000$, find the multiplicity of the smallest prime factor p in n, that is the largest exponent m for which

p^m divides n; prove that it is an additive function; is it completely additive?

6. For $n = 1, 2, 3, \ldots, 20, 100, 2000$, find the integer logarithm of n, i.e., the sum of primes dividing n counting multiplicity (the *potency* of n, or the *integer logarithm* of n); is this function additive? is it completely additive?
7. Prove that $f(n) = gcd(n, k)$ (the greatest common divisor of n and k), where k is a fixed integer, is a multiplicative function; is it completely multiplicative?
8. Let $1_C(n)$ is the indicator function of the set C containing 1: $1_C(n) = 1$ if $n \in C$, and $1_C(n) = 0$ otherwise. Find $1_C(1)$, $1_C(100)$, $1_C(1000)$, if $C = \{1, 2, \ldots, 10\}$; $C = \{2k - 1 | k \in \mathbb{N}\}$; $C = \{k^3 | k \in \mathbb{N}\}$. Prove that $1_C(n)$ is a completely multiplicative function.
9. Let $r_2(n)$ gives the number of representations of n as a sum of squares of two integers, positive, negative, or zero, where in counting the number of ways, reversal of order is allowed. Prove that $r_2(n)$ is not multiplicative but $\frac{r_2(n)}{4}$ is multiplicative.

2.2. Floor Function and Its Relatives

2.2.1. The *floor function* $\lfloor x \rfloor$, $x \in \mathbb{R}$, is defined as the largest integer less than or equal to a given real number x.

The function $\{x\}$, $x \in \mathbb{R}$, is the *fractional value* of a given real number x: $\{x\} = x - \lfloor x \rfloor$.

The *ceiling function* $\lceil x \rceil$, $x \in \mathbb{R}$, is defined as the smallest integer greater than or equal to x.

The function $||x|| = \min\{\{x\}, 1 - \{x\}\}$, $x \in \mathbb{R}$, is the distance between a given real number x and the integer closest to x.

For example, $\lfloor 2.9 \rfloor = 2$, $\lfloor -2 \rfloor = -2$, and $\lfloor -2.3 \rfloor = -3$; $\{2.9\} = 0.9$, $\{-2\} = 0$, and $\{-2.3\} = 0.7$; $\lceil 2.9 \rceil = 3$, $\lceil -2 \rceil = -2$, and $\lceil -2.3 \rceil = -2$; $||2.9|| = 0.1$, $|| - 2|| = 0$, and $|| - 2.3|| = 0.3$.

2.2.2. Consider a list of the simplest properties of floor function and its relatives.

Properties of floor function and its relatives

1. $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ for any real x; $\lfloor x \rfloor = x$ if and only if x is an integer.
2. $\lfloor k+x \rfloor = k + \lfloor x \rfloor$ for any integer number k and any real number x.
3. For any real x and any integer n, it holds that $n \leq x$ if and only if $n \leq \lfloor x \rfloor$.
4. $|\{n \in \mathbb{N} : n \leq x, d|n\}| = \left\lfloor \frac{x}{d} \right\rfloor$ for any positive real x and any positive integer d.
5. $\lfloor \lfloor x \rfloor \rfloor = \lfloor x \rfloor$ for any real x.
6. $\left\lfloor \frac{x}{d} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{d} \right\rfloor$ for any positive real x and any positive integer d.
7. $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$, where $x, y \in \mathbb{R}$.
8. $\lfloor x \rfloor - 2 \left\lfloor \frac{x}{2} \right\rfloor = 0$ or 1 for any real x.
9. $n! = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, where p_i are all prime numbers less than or equal to n, and
$$\alpha_i = \left\lfloor \frac{n}{p_i} \right\rfloor + \left\lfloor \frac{n}{p_i^2} \right\rfloor + \left\lfloor \frac{n}{p_i^3} \right\rfloor + \cdots .$$
10. $0 \leq \{x\} < 1$ for any real number x; $\{x\} = 0$ if and only if x is an integer.
11. $\{k + x\} = \{x\}$ for any integer number k for any real number x.
12. $||x|| = \lfloor x + 0.5 \rfloor$, where $x \in \mathbb{R}$.
13. $\lceil x \rceil = -\lfloor -x \rfloor$, where $x \in \mathbb{R}$.
14. $x \leq \lceil x \rceil < x + 1$, where $x \in \mathbb{R}$.
15. $\left\lfloor \frac{k}{2} \right\rfloor + \left\lceil \frac{k}{2} \right\rceil = k$, where $k \in \mathbb{Z}$.

□ Prove, for example, property 4. In order to prove the formula $|\{n \in \mathbb{N} : n \leq x, d|n\}| = \left\lfloor \frac{x}{d} \right\rfloor$, one can consider the numbers d, $2d$, $\ldots$, $kd \leq x < (k+1)d$. It is easy to see that

$$|\{n \in \mathbb{N} : n \leq x, d|n\}| = k.$$

On the other hand, it holds that $k \leq \frac{x}{d} < k + 1$, i.e., $k = \left\lfloor \frac{x}{d} \right\rfloor$. □

2.2.3. In this chapter, we are going to solve several important equations connected with the considered arithmetic functions.

For example, let us solve the equation $\lfloor x \rfloor = 1 + 2\{x\}$.

It is obvious that $1 + 2\{x\}$ is an integer, hence $\{x\} = 0$ or $\{x\} = 0.5$. In the first case, $\lfloor x \rfloor = 1$, i.e., $x = \lfloor x \rfloor + \{x\} = 1 + 0 = 1$. In the second case, $\lfloor x \rfloor = 2$, i.e., $x = \lfloor x \rfloor + \{x\} = 2 + 0.5 = 2.5$.

So, we find all solutions of the equation $\lfloor x \rfloor = 1 + 2\{x\}$: They are 1 and 2.5.

2.2.4. It is easy to show that for any continuous function $f(x)$, nonnegative on the segment $[a, b]$, the number of points (x, y) with positive integers x, y in the domain with the borders $x = a$, $x = b$, $y = 0$, and $y = f(x)$ is $\sum_{a \le x \le b} \lfloor f(x) \rfloor$, where the summation is over all integers x from the segment $[a, b]$.

In particular, the number of points (x, y) with positive integers x, y under the hyperbola $xy = n$ is

$$2 \sum_{0 < x \le \sqrt{n}} \left\lfloor \frac{n}{x} \right\rfloor - \left\lfloor \sqrt{n} \right\rfloor^2,$$

where the summation is over all positive integers x less than or equal n, $n \in \mathbb{N}$.

Such considerations lead to asymptotic formulas for mean values of well-known arithmetic functions. We use these and other considerations in Section 2.6.

For the detailed proofs of the above properties, examples of solutions to the problems, and some additional information, see, for example, [Buch09], [DeKo13], [Chan70], [Ingh32], and [Step01].

Exercises

1. How many positive integers less than 200 are not divisible on 2 and not divisible on 5? How many positive integers less than 100 are not divisible on 2, not divisible on 3, and not divisible on 5?
2. How many positive integers less than 300 are relatively prime to 225? How many positive integers less than 100 are relatively prime to 36? How many three-digit positive integers are relatively prime to 1000?

3. How many zeros are there in the end of the representation of n in the base g:

(a) $n = 1994!,\ g = 10;$
(b) $n = 200!,\ g = 10;$
(c) $n = 2010!,\ g = 6;$
(d) $n = 3000!,\ g = 60;$
(e) $n = 2004!,\ g = 12;$
(f) $n = 500!,\ g = 12;$
(g) $n = \frac{100!}{80!20!},\ g = 6;$
(h) $n = \frac{200!}{100!100!},\ g = 10;$
(i) $n = \frac{666!}{660!6!},\ g = 13;$
(j) $n = \frac{100!}{50!50!},\ g = 60;$
(k) $n = \frac{30!}{10!10!},\ g = 8;$
(l) $n = \frac{200!}{50!150!},\ g = 20?$

4. Is it true that:

(a) $500!$ is divisible by 22^{50};
(b) $100!$ is divisible by 30^{30};
(c) $\frac{200!}{100!100!}$ is divisible by 100^{10};
(d) $\frac{100!}{80!20!}$ is divisible by 20^{20}?

5. Solve the equation:

(a) $\lfloor x \rfloor = -3;$
(b) $\lfloor 2x \rfloor = 2;$
(c) $\left\lfloor x^2 - 4x + 7 \right\rfloor = 3;$
(d) $\left\lfloor 3x^2 - x \right\rfloor = x + 1;$
(e) $\{x\} = 0.2;$
(f) $\{3x\} = 0.9;$
(g) $\{x^2 + 5\} = 0;$
(h) $\{x\} = \lfloor x + 15 \rfloor;$
(i) $\lfloor x \rfloor + 5 = 2\{x\};$
(j) $\{x\} = \lfloor x \rfloor;$
(k) $\lfloor x \rfloor + 5 = \{x\};$
(l) $\frac{x-1}{3} = \{x\};$
(m) $\frac{x-3}{5} = 2\{x\};$
(n) $\frac{x+5}{4} = 3\{x\};$
(o) $\lfloor x \rfloor - 3\{x\} = 2x + 1;$
(p) $\lfloor x \rfloor + 2\{x\} = 2x - 1;$
(q) $\{x\} = 0.4;$
(r) $\{x + 5\} = 0.3;$
(s) $\lfloor x - 3 \rfloor = -3;$
(t) $\lfloor x + 3 \rfloor = 5;$
(u) $\left\lfloor 1 - x^2 \right\rfloor = 0;$
(v) $\left\lfloor x^2 - 2 \right\rfloor = -1;$
(w) $\lfloor \sin x \rfloor = -1;$
(x) $\lfloor \cos x \rfloor = 0;$
(y) $\lfloor \log x + 1 \rfloor = -1;$
(z) $\lfloor 2 - \log_3 x \rfloor = 4.$

6. Solve the inequality:

(a) $\left\lfloor 1 - x^2 \right\rfloor > -4;$
(b) $\{1 - x^2\} > 0.5;$
(c) $\lfloor \sin 2x - 4 \rfloor \le -3.5;$
(d) $\{\sin 2x - 4\} \le 0.5;$
(e) $\lfloor \log_5 x \rfloor \ge 0;$
(f) $\{\log_5 x\} \ge 0.2.$

7. Find:
   (a) $\lfloor x \rfloor - k\left\lfloor \frac{x}{k} \right\rfloor$, where $x \in \mathbb{R}$, $k \in \mathbb{N}$;
   (b) $\lfloor x \rfloor + \lfloor -x \rfloor$, where $x \in \mathbb{R}$.
8. Find $\lfloor \sqrt{1} \rfloor + \lfloor \sqrt{2} \rfloor + \cdots + \left\lfloor \sqrt{n^2+1} \right\rfloor$, where $n \in \mathbb{N}$.
9. Prove that $\lfloor x \rfloor + \lfloor x + 0.5 \rfloor = \lfloor 2x \rfloor$, where $x \in \mathbb{R}$.
10. Prove, that $\lfloor x \rfloor + \left\lfloor x + \frac{1}{k} \right\rfloor + \cdots + \left\lfloor x + \frac{k-1}{k} \right\rfloor = \lfloor kx \rfloor$, where $x \in \mathbb{R}$, $k \in \mathbb{N}$.
11. Prove that $\left\lfloor \frac{m}{n} \right\rfloor + \left\lfloor \frac{2m}{n} \right\rfloor + \cdots + \left\lfloor \frac{(n-1)m}{n} \right\rfloor = \frac{(m-1)(n-1)}{2}$, where $m, n \in \mathbb{N}, (m,n) = 1$.
12. Prove that $\sum_{m\geq 1}\left(\left\lfloor \frac{n}{m} \right\rfloor - \left\lfloor \frac{n-1}{m} \right\rfloor\right) = 2 \Leftrightarrow n \in P$.

2.3. Möbius Function

2.3.1. The *Möbius function* $\mu(n)$ is defined for any positive integer n, taking only the values $\{-1, 0, 1\}$: $\mu(n) = 1$ if n is square-free number with an even number of prime divisors; $\mu(n) = -1$ if n is square-free number with an odd number of prime divisors; $\mu(n) = 0$ if n is not a square-free number.

Recall that a *square-free integer* is an integer which is divisible by no perfect square other than 1. That is, its prime factorization has exactly one factor for each prime that appears in it. For example, $10 = 2 \cdot 5$ is square-free but $18 = 2 \cdot 3^2$ is not because 18 is divisible by $9 = 3^2$. The smallest positive square-free numbers are 1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 22,… (sequence A005117 in the OEIS).

In other words,

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ (-1)^s, & \text{if } n = p_1 \cdot \ldots \cdot p_s, \text{ where } p_i \in P, \\ & \quad \text{and } p_i \neq p_j \text{ for } i \neq j, \\ 0, & \text{if } \exists p \in P : p^2 | n. \end{cases}$$

For example, $\mu(6) = 1$, as $6 = 2 \cdot 3$ is a square-free number having two prime divisors; $\mu(70) = -1$, as $70 = 2 \cdot 5 \cdot 7$ is a square-free number having two prime divisors; $\mu(50) = 0$, as $50 = 2 \cdot 5^2$ is divisible by the square of a prime number 5 and hence is not square-free.

2.3.2. Consider some properties of the Möbius function, which are important for our further consideration.

Properties of the Möbius function

1. The Möbius function is multiplicative, i.e., it holds that $\mu(1) = 1$, and $\mu(m \cdot n) = \mu(m) \cdot \mu(n)$ for any coprime positive integers n and m.
2. $\sum_{d|n} \mu(d) = 1$ for $n = 1$, and $\sum_{d|n} \mu(d) = 0$ for $n > 1$.
3. $F(n) = \sum_{d|n} f(d)$ if and only if $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$ (*Möbius inversion formula*).
4. $\sum_{d|n} \frac{\mu(d)}{d} = 1$ for $n = 1$, and $\sum_{d|n} \mu(d) d = \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right)$ for $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$.

☐ 1. The first property is obvious. It should be checked only in the case of two coprime square-free numbers n and m. But in this case, $n = p_1 \cdot \ldots \cdot p_s$, $m = q_1 \cdot \ldots \cdot q_t$, $p_i \neq q_j$, and we have

$$\mu(n \cdot m) = \mu(p_1 \cdot \ldots \cdot p_s \cdot q_1 \cdot \ldots \cdot q_t) = \mu(p_1 \cdot \ldots \cdot p_s) \cdot \mu(q_1 \cdot \ldots \cdot q_t) = \mu(n) \cdot \mu(m).$$

2. In order to prove the second property, note that $\sum_{d|1} \mu(d) = \mu(1) = 1$. If $n \neq 1$, then $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, and

$$\sum_{d|n} \mu(d) = \prod_{i=1}^{s} (1 + \mu(p_i) + \mu(p_i^2) + \cdots + \mu(p_i^{\alpha_i}))$$
$$= \prod_{i=1}^{s} (1 - 1 + 0 + \cdots + 0) = 0.$$

3. The proof of the Möbius inversion formula is as follows:

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} f(c)$$
$$= \sum_{cd|n} \mu(d) f(c) = \sum_{c|n} f(c) \sum_{d|\frac{n}{c}} \mu(d) = f(n).$$

On the other hand,

$$\sum_{d|n} f(d) = \sum_{d|n}\sum_{c|d} \mu(c)F\left(\frac{d}{c}\right) = \sum_{k|n} F(k)\sum_{c} \frac{n}{k}\mu(c) = F(n).$$

4. As the functions $f_1(n) = \mu(n)$ and $f_2(n) = \frac{1}{n}$ are multiplicative, the function $f(n) = \frac{\mu(n)}{n}$ is multiplicative as the product of the functions $f_1(n)$ and $f_2(n)$. Then,

$$\sum_{d|n} f(d) = \prod_{i=1}^{s}(1 + f(p_i) + f(p_i^2) + \cdots + f(p_i^{\alpha_i}))$$

for $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. In other words,

$$\sum_{d|n} \frac{\mu(d)}{d} = \prod_{i=1}^{s}\left(1 + \frac{\mu(p_i)}{p_i} + \frac{\mu(p_i^2)}{p_i^2} + \cdots + \frac{\mu(p_i^{\alpha_i})}{p_i^{\alpha_i}}\right)$$
$$= \prod_{i=1}^{s}\left(1 - \frac{1}{p_i} + 0 + \cdots + 0\right).$$

So, for $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, we have the formula $\sum_{d|n} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot (1 - \frac{1}{p_s})$. For $n = 1$, the result is obvious. $\square$

The classic Möbius inversion formula was introduced into number theory during the 19th century by the German mathematician and theoretical astronomer, August Ferdinand Möbius (1790–1868). The Möbius inversion formula is also correct if F and f are functions from the positive integers into some abelian group. In the language of the Dirichlet convolution $*$, the equality $F(n) = \sum_{d|n} f(d)$ may be written as $F = f * 1$, where 1 is the constant function: $1(n) = 1$ for any positive integer. The $f(n) = \sum_{d|n} \mu(d)F\left(\frac{n}{d}\right)$ is then written as $f = F * \mu$. So, the Möbius inversion formula takes the form

$$F = f * 1 \Leftrightarrow f = F * \mu.$$

2.3.3. Consider some equations involving the Möbius function.

For solving the equation $\mu(2x) = \mu(3x)$, $x \in [1, 20]$, consider positive integer x as $x = 2^\alpha 3^\beta y$, where α and β are non-negative integers, and the positive integer y is not divisible by 2 and 3, i.e.,

$(2, y) = (3, y) = 1$. In this case, $\mu(2x) = \mu(2^{\alpha+1})\mu(3^{\beta})\mu(y)$ and $\mu(3x) = \mu(2^{\alpha})\mu(3^{\beta+1})\mu(y)$. If $\mu(y) = 0$, i.e., if y is divisible by the square of a prime number, this equality holds. If $\mu(y) \neq 0$, i.e., if y is square-free, we obtain the equation $\mu(2^{\alpha+1})\mu(3^{\beta}) = \mu(2^{\alpha})\mu(3^{\beta+1})$.

If $\alpha > 1$ or $\beta > 1$, then we obtain $0 = 0$.

If $\alpha = 0$ and $\beta = 0$, then we obtain $\mu(2) = \mu(3)$, i.e., $-1 = -1$.

If $\alpha = 0$, $\beta = 1$, then we obtain $1 = 0$, a contradiction.

If $\alpha = 1$, $\beta = 0$, then we obtain $0 = 1$, a contradiction.

If $\alpha = 1$ and $\beta = 1$, we obtain $0 = 0$.

So, the set of solutions of the equation $\mu(2x) = \mu(3x)$ is formed by all positive integers except square-free numbers of the forms $2y$ or $3y$, where $(y, 2) = (y, 3) = 1$. In the segment from 1 to 20, they are 2, 3, 10, 14, and 15.

So, all solutions of the equation $\mu(2x) = \mu(3x)$ on the segment $[1, 20]$ are 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 16, 17, 18, 19, and 20.

For the proofs of these and other properties, examples of solutions of problems, and some additional information, see, for example, in [Apos86], [Buch09], [DeKo13], [Gaus01], [HaWr79], [MSC96], and [Wiki22].

Exercises

1. Calculate:

   (a) $\mu(65)$; (c) $\mu(91)$; (e) $\mu(68)$; (g) $\mu(242)$;
   (b) $\mu(66)$; (d) $\mu(330)$; (f) $\mu(135)$; (h) $\mu(250)$.

2. Calculate:

   (a) $\mu(\sigma(14))$; (b) $\mu(\tau(10)!)$; (c) $\mu(\phi(15))$; (d) $\mu(\frac{10!}{5!5!})$.

3. Solve the equation:

   (a) $\mu(5x) = \mu(3x)$, $x \in [5, 25]$; (c) $\mu(3x) = \mu(7x)$, $x \in [40, 70]$;
   (b) $\mu(2x) = \mu(7x)$, $x \in [10, 30]$; (d) $\mu(5x) = \mu(7x)$, $x \in [40, 60]$.

4. Check the identity $\sum_{d|n} \mu(d)\sigma(\frac{n}{d}) = n$ for $n \in \{1, 5, 10, 20\}$; prove it for any positive integer n.

5. Find the values of *Mertens function* $M(n) = \sum_{i=1}^{n} \mu(n)$ for all $n \in \{1, 2, \ldots, 20\}$.
6. Let $\nu(n)$ be the number of distinct prime divisors of a positive integer n and $\Omega(n)$ be the number of all possible prime divisors of n, counting with repetitions. Prove that $\mu(n) = (-1)^{\nu(n)} = (-1)^{\Omega(n)}$ if $\nu(n) = \Omega(n)$ and $\mu(n) = 0$ otherwise.
7. Find the sum:

   (a) $\sum\limits_{d|n} \frac{\mu(d)}{d}$;

   (b) $\sum\limits_{d|n} \frac{n\mu(d)}{d}$;

   (c) $\sum\limits_{d|n} \mu\left(\frac{n}{d}\right)(-7)^{\nu(d)}$;

   (d) $\sum\limits_{d|n} \mu(d)3^{\nu(d)}$;

   (e) $\sum\limits_{d|n} \mu\left(\frac{n}{d}\right)(-3)^{\nu(d)}$;

   (f) $\sum\limits_{d|n} \mu(d)2^{\nu(d)}$.
8. Prove that $\sum_{d|n} |\mu(d)| = 2^{\nu(n)}$.

2.4. Euler's Totient Function

2.4.1. For a given positive integer n, the *Euler's totient function* $\phi(n)$ is defined as the number of positive integers less than or equal to n and coprime to n:

$$\phi(n) = |\{x \in \mathbb{N} : x \leq n, (x, n) = 1\}|.$$

For example, $\phi(8) = 4$, as there exist exactly four positive integers less than 8 and coprime with 8: 1, 3, 5, and 7.

2.4.2. Consider a list of well-known properties of the Euler's totient function.

Properties of the Euler's totient function

1. $\phi(p) = p - 1$ for any prime p.
2. $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$ for any prime p and any positive integer α.
3. The Euler's totient function is multiplicative, i.e., $\phi(1) = 1$, and $\phi(mn) = \phi(m)\phi(n)$ for any coprime positive integers m and n.
4. $\phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = p_1^{\alpha_1-1} \cdot p_2^{\alpha_2-1} \cdot \ldots \cdot p_s^{\alpha_s-1}(p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_s - 1)$, where $p_1, \ldots, p_s$ are distinct prime numbers and $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$.

5. $\sum_{d|n} \phi(d) = n$ (*Gauss identity*).
6. $\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$.
7. $\sum_{\phi(d)=n} \mu(d) = 0$.

□ The first property is obvious, as from p positive integers less than p, only p itself is not coprime with p.

Similarly, from p^α positive integers $1, 2, \ldots, p^\alpha$, there are exactly $p^{\alpha-1}$ numbers (in fact, p, p^2, $p^3, \ldots, p^\alpha$) not coprime with p^α.

To prove the multiplicativity of the Euler's totient function, we consider two relatively prime numbers m and n and make a rectangular table of the numbers 1 to mn with m rows and n columns as follows:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ 3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ m & 2m & 3m & \cdots & nm. \end{array}$$

The numbers in the rth row of this table are of the form $km + r$ as k runs from 0 to $m - 1$.

Let $d = gcd(r, m)$. If $d > 1$, then no number in the rth row of the table is relatively prime to mn since $d|(km + r)$ for all k. So, to count the residues relatively prime to mn, we need only to look at the rows indexed by values of r such that $gcd(r, m) = 1$, and there are $\phi(m)$ such rows. If $gcd(r, m) = 1$, then every entry in the rth row is relatively prime to m since $gcd(km + r, m) = 1$ by the Euclidean algorithm. The entries in this row form a complete residue system modulo n (see Chapter 1). Thus, exactly $\phi(n)$ of them will be relatively prime to n and thus relatively prime to mn.

We have shown that there are $\phi(m)$ rows in the table which contain numbers relatively prime to mn, and each of those contain exactly $\phi(n)$ such numbers. So, there are, in total, $\phi(m)\phi(n)$ numbers in the table which are relatively prime to mn. This proves the result.

Property 4 follows now from properties 2 and 3. It can be rewritten in the following form:

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right)$$

for $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$. As for property 6, we can see that $(1 - \frac{1}{p_2}) \cdot \ldots \cdot (1 - \frac{1}{p_s}) = \frac{\phi(n)}{n}$ for $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$; so, we get the formula $\sum_{d|n} \frac{\mu(d)}{d} = \frac{\phi(n)}{n}$; it follows now from property 4 of the Möbius function. □

2.4.3. Consider some equations connected with the Euler's totient function.

Let us solve the equation $\phi(x) = \frac{x}{3}$.

It is obvious that $x \neq 1$. In this case, x has a prime decomposition $x = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, and $\phi(x) = x(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k})$. In other words, we get the equation $(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}) = \frac{1}{3}$. Considering all possible multipliers $\frac{1}{2}, \frac{2}{3}, \frac{4}{5}, \frac{6}{7}, \ldots$ of the left part of the equation, we can see that the fraction $\frac{1}{3}$ can be obtained only as the product of the fractions $\frac{1}{2}$ and $\frac{2}{3}$. So, $x = 2^\alpha \cdot 3^\beta$, where $\alpha, \beta \in \mathbb{N}$.

Solve the equation $\phi(2x) = \phi(3x)$.

Consider a positive integer x as $x = 2^\alpha 3^\beta y$, where α and β are non-negative positive integers, and positive integer y is not divisible by 2 and by 3, i.e., $gcd(2, y) = gcd(3, y) = 1$. In this case,

$$\phi(2x) = \phi(2^{\alpha+1})\phi(3^\beta)\phi(y), \quad \phi(3x) = \phi(2^\alpha)\phi(3^{\beta+1})\phi(y),$$

and the equation $\phi(2x) = \phi(3x)$ obtains the form $\phi(2^{\alpha+1})\phi(3^\beta) = \phi(2^\alpha)\phi(3^{\beta+1})$.

As $\phi(2^{\alpha+1}) = 2^\alpha$ and $\phi(3^{\beta+1}) = 2 \cdot 3^\beta$, we obtain the equation $2^\alpha\phi(3^\beta) = 2 \cdot 3^\beta\phi(2^\alpha)$.

If $\alpha = 0$, $\beta = 0$, then we get $1 = 2$, a contradiction.

If $\alpha = 0$, $\beta \neq 0$, then we get $2 \cdot 3^{\beta-1} = 2 \cdot 3^\beta$, a contradiction.

If $\alpha \neq 0$, $\beta = 0$, then we get the identity $2^\alpha = 2 \cdot 2^{\alpha-1}$, which is true for all such α and β.

If $\alpha \neq 0$, $\beta \neq 0$, we get $2^\alpha \cdot 2 \cdot 3^{\beta-1} = 2 \cdot 3^\beta \cdot 2^{\alpha-1}$, a contradiction.

So, the set of all solutions of the equation $\phi(2x) = \phi(3x)$ consists of the positive integers of the form $2^\alpha y$, where $\alpha \in \mathbb{N}$, and positive integer y is not divisible by 2 and 3, i.e., is coprime with 6.

Solve the equation $\phi(x) = 2$.

It is obvious that $x \neq 1$. In this case, $x = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, and

$$\phi(x) = p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1).$$

Let $\phi(x) = 2^m l$, where l is an odd number. As for an odd prime number p, the number $p - 1$ is even, we get that in the prime decomposition of x, there is less than or equal to m odd prime multipliers. In other words, $k \leq m + 1$. Moreover, if $k = m + 1$, then $p_1 = 2$.

In our case, $m = 1$, i.e., $k \leq 2$, and if $k = 2$, then $p_1 = 2$.

Let $k = 1$, i.e., $x = p^\alpha$.

If $p = 2$, then $\phi(x) = \phi(2^\alpha) = 2^{\alpha-1}$, and we get the equation $2^{\alpha-1} = 2$. In this case, $\alpha = 2$ and $x = 2^2 = 4$.

If $p \neq 2$, then $\phi(x) = \phi(p^\alpha) = p^{\alpha-1}(p-1)$, and we get the equation $p^{\alpha-1}(p - 1) = 2$. In this case, $p - 1 = 2$ and $p^{\alpha-1} = 1$. So, $p = 3$, $\alpha = 1$, and $x = 3$.

Let $k = 2$, i.e., $x = 2^\alpha p^\beta$.

Then, $\phi(x) = \phi(2^\alpha p^\beta) = 2^{\alpha-1}p^{\beta-1}(p-1)$, and we get the equation $2^{\alpha-1}p^{\beta-1}(p-1) = 2$. In this case, $p-1 = 2$, $2^{\alpha-1} = 1$ and $p^{\beta-1} = 1$. So, $p = 3$, $\alpha = \beta = 1$, and $x = 2 \cdot 3 = 6$.

Therefore, we get all the solutions to the equation $\phi(x) = 2$: the positive integers 3, 4, and 6.

2.4.4. A *totient number* is a value of the Euler's totient function: that is, an m for which there is at least one n such that $\phi(n) = m$. The *valency* (or *multiplicity*) of a totient number m is the number of solutions to this equation.

As the equation $\phi(x) = 2$ has exactly three solutions, 3, 4, and 6, we get that 2 is a totient number of valency 3.

The following sequence presents for $n = 1, 2, 3, \ldots$ values $\phi(n)$, i.e., count numbers less then or equal to n and coprime to n. So, it presents all totient numbers with their valencies: 1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4, 12, 6, 8, … (sequence A005277 in the OEIS).

It is easy to see that

- *there are infinitely many totient numbers.*

☐ In fact, all numbers of the form $p-1$, $p \in P$ are totient, as $\phi(p)=p-1$. ☐

Also,

- *a pronic number $p(p-1)$ with prime p is totient.*

☐ It is certainly true since $\phi(p^2)=p(p-1)$. ☐

Moreover, it is easy to show that

- *if n is a totient, then $n \cdot 2^k$ is a totient for all positive integers k.*

☐ In fact, if an odd m is a solution to the equation $\phi(x)=n$, then $2^{k+1}m$ is a solution to the equation $\phi(x)=n \cdot 2^k$. If an even m is a solution to the equation $\phi(x)=n$, then $m=2^t l$ with odd l. It is easy to see that in this case, $2^{k+1}m=2^{k+t+1}l$ is a solution to the equation $\phi(x)=n \cdot 2^k$. ☐

Ford (1999, [Ford99]) proved that

- *for every integer $k \geq 2$, there is a totient number m of multiplicity k.*

That is, for every integer $k \geq 2$, there exists a number m for which the equation $\phi(n)=m$ has exactly k solutions. This result had previously been conjectured by Wacław Sierpiński.

However, no number m is known with multiplicity $k=1$. *Carmichael's totient function conjecture* is the statement that there is no such m.

2.4.5. A *non-totient number* is a positive integer which is not totient, i.e., it is not in the range of the Euler's totient function. That is, the equation $\phi(x)=n$ has no solution. In other words, n is a non-totient if there is no integer x that has exactly n coprimes below it.

For example, one can easily check that the equation $\phi(x)=3$ has no solution, so the number 3 is non-totient.

The first few non-totient numbers are 3, 5, 7, 9, 11, 13, 14, 15, 17, 19, 21, 23, 25, 26, 27, ... (sequence A007617 in the OEIS).

It is easy to see that

- *all odd numbers are non-totients except* 1.

□ Since the equation $\phi(n) = 1$ has the solutions $x = 1$ and $x = 2$, the number 1 is totient. For all positive integers $n \geq 3$ the value $\phi(n)$ is even; if there is an odd prime p, divided by n, then $p - 1$ divides $\phi(n)$; otherwise, $n = 2^{\alpha}$, $\alpha \geq 2$, and $2^{\alpha-1}$ divides $\phi(n)$. □

As the simple consequence of this fact, we can state that

- *there are infinitely many non-totient numbers.*

However, there are also even non-totients, the first is 14. Moreover, it is proven ([Zhan93], [MSC96]) that

- *there are infinitely many even non-totients,*

and indeed,

- *every positive integer has a multiple which is an even non-totient.*

The first few even non-totients are 14, 26, 34, 38, 50, 62, 68, 74, 76, 86, 90, 94, 98, 114, 118, ... (sequence A005277 in the OEIS).

For more information, we list the following sequences:

- the least k such that the totient of k is n for $n = 1, 2, 3, \ldots$ are (0 if no such k exists) 1, 3, 0, 5, 0, 7, 0, 15, 0, 11, 0, 13, 0, 0, 0, ... (sequence A049283 in the OEIS);
- the greatest k such that the totient of k is n for $n = 1, 2, 3, \ldots$ are (0 if no such k exists) 2, 6, 0, 12, 0, 18, 0, 30, 0, 22, 0, 42, 0, 0, 0, ... (sequence A057635 in the OEIS);
- the number of ks such that $\phi(k) = n$ for $n = 1, 2, 3, \ldots$ are 2, 3, 0, 4, 0, 4, 0, 5, 0, 2, 0, 6, 0, 0, 0, ... (sequence A014197 in the OEIS); according to Carmichael's conjecture, there are no ones in this sequence.

2.4.6. A *cototient number* is a positive integer n that can be expressed as the difference between a positive integer m and the number of coprime integers below it. That is, the equation $x - \phi(x) = n$ has at least one solution.

It is easy to check that 1 is cototient, as $\phi(p) = p - 1$ and hence $p - \phi(p) = 1$; so, the valency of 1 is the infinity. As $\phi(4) = 2$, then 4 is cototient.

The following sequence presents for $n = 1, 2, 3, \ldots$ values $n - \phi(n)$, i.e., all cototient numbers with heir valencies: 0, 1, 1, 2, 1, 4, 1, 4, 3, 6, 1, 8, 1, 8, 7, ... (sequence A051953 in the OEIS).

2.4.7. A *non-cototient number* is a positive integer n that cannot be expressed as the difference between a positive integer m and the number of coprime integers below it. That is, the equation $x - \phi(x) = n$ has no solution.

It is easy to check that the smallest non-cototient number is 10. The sequence of non-cototients starts from 10, 26, 34, 50, 52, 58, 86, 100, 116, 122, 130, 134, 146, 154, 170, ... (sequence A005278 in the OEIS).

It is conjectured that

- *all non-cototients are even.*

This can follow from a modified form of the slightly stronger version of the *Goldbach conjecture*: If the even number n can be represented as a sum of two distinct primes p and q, then

$$pq - \phi(pq) = pq - (p - 1)(q - 1) = p + q - 1 = n - 1.$$

It is expected that every even number larger than 6 is a sum of two distinct primes, so probably *no odd number larger than 5 is a non-cototient.* The remaining odd numbers are covered by the observations

$$1 = 2 - \phi(2), \quad 3 = 9 - \phi(9), \quad 5 = 25 - \phi(25).$$

For even numbers, it can be shown that

$$2pq - \phi(2pq) = 2pq - (p - 1)(q - 1) = pq + p + q - 1 = (p + 1)(q + 1) - 2.$$

Thus,

- *all even numbers n such that $n + 2$ can be written as $(p + 1)(q + 1)$, where p, q primes are cototients.*

For more information, we list the following sequences:

- the least ks such that the cototient of k is n for $n = 1, 2, 3, \ldots$ are (0 if no such k exists) 1, 2, 4, 9, 6, 25, 10, 15, 12, 21, 0, 35, 18, 33, 26, ... (sequence A063507 in the OEIS);
- the greatest ks such that the cototient of k is n for $n = 1, 2, 3, \ldots$ are (0 if no such k exists) ∞, 4, 9, 8, 25, 10, 49, 16, 27, 0, 121, 22, 169, 26, 55, ... (sequence A063748 in the OEIS);
- the number of ks such that $k - \phi(k)$ is n for $n = 1, 2, 3, \ldots$ are ∞, 1, 1, 2, 1, 1, 2, 3, 2, 0, 2, 3, 2, 1, 2, ... (sequence A063740 in the OEIS).

Erdős (1913–1996) and Sierpiński (1882–1969) asked

- *whether there exist infinitely many non-cototients.*

This was finally answered in the affirmative by Browkin and Schinzel (1995, [BrSc95]), who showed that every member of the infinite family $2^k \cdot 509203$ is an example (509203 is the first *Riesel number*). Since then, other infinite families of roughly the same form have been given by Flammenkamp and Luca (2000, [FlLu00]).

For additional proofs, examples of solutions of similar problems, and some other facts, see, for example, in [AbSt72], [BrSc95], [Buch09], [CoGu96], [DeKo13], [DeKo18], [Dick05], [Ford99], [FlLu00], [Gaus01], [GKP94], [Guy94], [HaWr79], [Lege79], [Ribe96], [Ore48], [Sloa22], and [Wiki22].

Exercises

1. How many zeros are there in end of the representation of the given number n in the base g:

   (a) $n = \phi(528)!,\ g = 15$;
   (b) $n = \phi(30)!,\ g = 12$;
   (c) $n = \phi(\phi(13))!,\ g = 14$;
   (d) $n = \phi(4!)!,\ g = 20$;
   (e) $\phi(528)!\ g = 12$;
   (f) $\phi(400)!\ g = 48$.

2. Find the number of positive integers n less than 200 such that $(n, 200) = 4$. Find the number of positive integers n less than 500

such that $(n, 500) = 10$. Find the number of positive integers n less than or equal 1000 and coprime with 77.

3. Find the number of positive integers n less than or equal $2^{30} - 1$ and coprime with $2^{10} - 1$. Find the number of positive integers n less than or equal to $8!$ and coprime with $6!$
4. Find the number of all proper simple non-reducted fractions with the denominator:

   (a) 90;
   (b) 114;
   (c) $12!$;
   (d) $15!$;
   (e) p, where $p \in P$.

5. Find the number of all proper simple non-reducted fractions with the denominator n dividing 2002?
6. Solve the equation:

   (a) $\phi(x) = \frac{2x}{3}$;
   (b) $\phi(x) = \frac{4x}{11}$;
   (c) $\phi(x) = \frac{x}{6}$;
   (d) $\phi(x) = \frac{x}{12}$;
   (e) $7\phi(x) = 4x$;
   (f) $7\phi(x) = 3x$;
   (g) $7\phi(x) = 2x$;
   (h) $15\phi(x) = 4x$;
   (i) $\phi(2x) = \phi(5x)$;
   (j) $\phi(3x) = \phi(5x)$;
   (k) $\phi(13x) = \phi(17x)$;
   (l) $\phi(2x) = \phi(31x)$;
   (m) $\phi(x) = 6$;
   (n) $\phi(x) = 10$;
   (o) $\phi(x) = 3$;
   (p) $\phi(x) = 4$;
   (q) $\phi(x) = 8$;
   (r) $\phi(x) = 12$;
   (s) $\phi(x) = 14$;
   (t) $\phi(x) = 16$;
   (u) $\phi(x) = 20$;
   (v) $\phi(x) = 24$;
   (w) $\phi(x) = 40$;
   (x) $\phi(x) = 50$.

7. Find all even positive integers $n \leq 50$ such that the equation $\phi(x) = n$ has no solutions.
8. Solve the equation $\phi(px) = \phi(qx)$ if p and q are distinct prime numbers. Solve the equation $\phi(x) = \frac{(p-1)x}{p}$ if p is a prime number.
9. Find a positive integer n if $n = 3^\alpha \cdot 5^\beta$, and $\phi(n) = 600$. Find a positive integer n if $\phi(7^n) = 705894$; if $\phi(3^n) = 162$.

10. Prove:
    (a) $\phi(4n) = 2\phi(2n)$;
    (b) $\phi(4n+2) = \phi(2n+1)$;
    (c) $n > 1 \Rightarrow 4|\phi(n^2+1)$;
    (d) $a|b \Rightarrow \phi(a)|\phi(b)$;
    (e) $(a,b) = d \Rightarrow \frac{\phi(ab)}{\phi(a)\phi(b)} = \frac{d}{\phi(d)}$;
    (f) $(a,b) > 1 \Rightarrow \phi(a)\phi(b) < \phi(ab)$;
    (g) $s \geq t \geq 1 \Rightarrow \frac{\phi(a^s)}{\phi(a^t)} = a^{s-t}$;
    (h) $p, 2p+1 \in P \Rightarrow \phi(4p+2) = \phi(4p) + 2$;
    (i) $\sum_{k=1}^{n} \phi(k)\lfloor \frac{n}{k} \rfloor = \frac{n(n+1)}{2}$;
    (j) $\sum_{k=1}^{n}(n,k) = \sum_{d|n} d\phi(\frac{n}{d})$.

2.5. Prime Counting Functions

Prime numbers

2.5.1. Any natural number p which has exactly two natural divisors is called a *prime number* or simply a *prime*.

The set of prime numbers is denoted by P. So, $P = \{2,3,5,7,11,13,17,19,23,29,\dots\}$.

A natural number n which has more than two natural divisors is called a *composite number*.

The set of composite numbers is denote as S. So, $S = \{4,6,8,9,10,12,14,15,16,18,\dots\}$.

As the unity has exactly one positive integer divisor, i.e., neither prime nor composite, we obtain that $\mathbb{N} = P \cup S \cup \{1\}$.

2.5.2. Over two thousand years ago, Euclid showed that

- *there are infinitely many prime numbers.*

The Euclid's proof is as follows.

□ Suppose that there are only finite number of primes, and $P = \{p_1,\dots,p_k\}$ are all the primes. Let $E = p_1 \dots p_k + 1$ and let p be a prime dividing E. Then, p cannot be any of $p_1,\dots,p_k$, otherwise

p would divide the difference $E - p_1 \dots p_k = 1$, which is impossible. So, this prime p is still another prime, and $p_1, \dots, p_k$ would not be all the primes. □

Euler gave an analytic proof of this fact.

□ In fact, if $P = \{p_1, \dots, p_k\}$ are all the primes, consider the rational number $X = \prod_{i=1}^{k}(1 - \frac{1}{p_i})^{-1}$. As the value $(1 - \frac{1}{p_i})^{-1}$ is the sum $1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots$ of infinite geometric progression $1, \frac{1}{p_i}, \frac{1}{p_i^2}, \dots$, we obtain that

$$\begin{aligned}\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)^{-1} &= \prod_{i=1}^{k}\left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots\right) \\ &= \sum_{\alpha_i \geq 0} \frac{1}{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} = \sum_{n=1}^{\infty} \frac{1}{n}.\end{aligned}$$

But $\sum_{n=1}^{\infty} \frac{1}{n}$ is the harmonic series, which is divergent, a contradiction. □

Primes are more than just oddities: They have become extremely important in cryptography because it is difficult to factor a large composite number into primes. In fact, for general numbers that are a few hundred decimal digits long, factorization is nearly impossible; this gave rise to the *RSA cryptosystem*.

How to recognize whether a natural number is a prime?

> *The problem of distinguishing prime n from composite numbers is known to be one of the most important and useful in Arithmetic.*
>
> — Gauss, 1801

2.5.3. An easy method of finding consecutive prime numbers was given by the Greek mathematician Eratosthenes.

We consider the sequence 2, 3, 4, ... Then, since 2 is the first prime number p_1, we remove from the sequence all the numbers greater than p_1 and divisible by p_1, i.e., starting with 2, each second number of the table. The first of the remaining numbers is $3 = p_2$.

Now, we remove all the numbers greater than p_2 and divisible by p_2, i.e., starting with 3, each third number of the table. The first of the reminding numbers is $5 = p_3$ and so on. Thus, we obtain $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11, \ldots$, $p_{1000} = 7917$, $p_{6000000} = 104395301, \ldots$. Here, p_n means the nth prime number.

Modern sieves include the *Brun sieve*, the *Selberg sieve*, and the *large sieve.*

2.5.4. A *primality test* is a test to determine whether or not a given number is prime, as opposed to actually decomposing the number into its constituent prime factors (which is known as *prime factorization*).

The simplest primality test is as follows: Given an integer n, we see if any integer m from 2 to $n-1$ divides n. If n is divisible by any m, then n is composite, otherwise it is prime.

Rather than testing all m up to $n-1$, we need only test m up to $\sqrt{n}$: If n is composite, then it has a prime divisor $p \leq \sqrt{n}$.

A good way to speed up these methods (and all the others mentioned in the following) is to precompute and store a list of all primes up to a certain bound (such a list can be computed with the Sieve of Eratosthenes). Then, before testing n for primality with a serious method, one first checks whether n is divisible by any prime from the list.

Primality tests come in two varieties: *deterministic* and *probabilistic.*

Deterministic tests determine with absolute certainty whether a number is prime. Examples of deterministic tests include the Lucas–Lehmer test and elliptic curve primality proving.

Probabilistic tests can potentially (although with very small probability) falsely identify a composite number as prime (although not vice versa).

Most popular primality tests are probabilistic tests. These tests use, apart from the tested number n, some other numbers a which are chosen at random from some sample space; the usual randomized primality tests never report a prime number as composite, but it is possible for a composite number to be reported as prime. The probability of error can be reduced by repeating the test with several independently chosen as.

2.5.5. The simplest probabilistic primality test is the *Fermat primality test.* It is only a heuristic test; some composite numbers (*Carmichael numbers*) will be declared probably prime no matter what witness is chosen. Nevertheless, it is sometimes used if a rapid screening of numbers is needed, for instance in the key generation phase of the RSA public key cryptographical algorithm.

The Fermat primality test uses the Fermat's little theorem.

Theorem (Fermat's little theorem). *If p is a prime and a is an integer coprime to p, then*

$$a^{p-1} \equiv 1(mod\ p).$$

□ Let us prove this theorem by induction.

For $a = 1$, one has $1^p \equiv 1(mod\ p)$.

Going from a to $a + 1$, we obtain

$$(a+1)^p \equiv a^p + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a + 1 \equiv a + 1(mod\ p),$$

as the binomial coefficients $\binom{p}{k} \equiv 0(mod\ p)$ for $k = 1, \ldots, p-1$. □

In fact, if we want to test if n is prime, then we can pick random a in the interval $[2, n-1]$ and see if the equality holds. If the equality does not hold for a value of a, then n is composite. If the equality does hold for many values of a, then we can say that n is a *probably prime* or a *pseudoprime.*

More exactly, a composite number x is called a *Fermat pseudoprime* to base a if the number a is coprime to x, and it holds that $a^{x-1} \equiv 1(mod\ x)$.

A *Poulet number* is a Fermat pseudoprime to base 2.

The smallest Poulet number is 341. It is not a prime since it holds $341 = 11 \cdot 31$, but it satisfies Fermat's little theorem: $2^{340} \equiv 1(mod\ 341)$.

The first few Poulet numbers are 341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, ... (sequence A001567 in the OEIS).

A number x that is a pseudoprime for all values of a that are coprime to x is called a *Carmichael number*.

In fact, a positive composite integer n is a Carmichael number if and only if n is square-free, and for all prime divisors p of n, it is true that $p - 1$ divides $n - 1$ (Korselt, 1899).

Korselt was the first who observed these properties, but he could not find an example. In 1910, Carmichael found the first and smallest such number, 561. (That 561 is a Carmichael number can be seen with Korselt's theorem. Indeed, $561 = 3 \cdot 11 \cdot 17$ is square-free and $2|560, 10|560,\ 16|560$.)

The next few Carmichael numbers are: $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, $2465 = 5 \cdot 17 \cdot 29$, $2821 = 7 \cdot 13 \cdot 31$, $6601 = 7 \cdot 23 \cdot 41$, and $8911 = 7 \cdot 19 \cdot 67$. (See sequence A002997 in the OEIS.)

There exist infinitely many Carmichael numbers (Alford, Granville, and Pomerance, 1994). Specifically, for sufficiently large n, there are at least $n^{2/7}$ Carmichael numbers between 1 and n. This makes tests based on Fermat's little theorem slightly risky.

Still, as numbers become larger, Carmichael numbers become very rare. For example, there are 1401644 Carmichael numbers between 1 and 10^{18} (approximately one in 700 billion numbers).

2.5.6. The *Solovay–Strassen primality test*, developed by Robert M. Solovay and Volker Strassen, is a probabilistic test to determine if a number is composite or probably prime.

Euler proved that

- *for a prime number p and any $a \in [1, p-1]$, it holds that*
$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (mod\ p),$$
where $\left(\frac{a}{p}\right)$ is the Legendre symbol.

The *Jacobi symbol* $\left(\frac{a}{n}\right)$, defined by
$$\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right)^{\alpha_i} \quad \text{for odd} \quad n = \prod_i p_i^{\alpha_i},$$
is a generalization of the Legendre symbol; here, n can be an arbitrary odd integer. The Jacobi symbol can be computed in time $O((\log n)^2)$ using the *law of quadratic reciprocity*.

Thus, if we have a value n and want to determine if it is prime, we can check many random values of a and make sure the above equality holds. If it does not hold for some a, we know that n must not be prime. Much like with the Fermat primality test, however, there are liars.

A value a is known as an *Euler liar* if the congruence $(\frac{a}{n}) \equiv a^{\frac{n-1}{2}} (mod\ n)$ holds, but n is composite.

Unlike the Fermat primality test, for every composite n at least half of all $a \in [1, p-1]$ are Euler witnesses. Therefore, there are no such values that are guaranteed to be liars all the time like Carmichael numbers are for Fermat test.

So, the test declares a composite n as probably prime with a probability at most 2^{-k}, where k is the number of different values of a we test.

2.5.7. Just like with the Fermat and Solovay–Strassen tests, with the *Miller–Rabin test*, we rely on an equality or a set of equalities that hold true for prime values and then see whether or not they hold for a number that we want to test for primality.

The original version of the Miller–Rabin primality test, due to G. L. Miller, was deterministic, but it relies on the unproven *generalized Riemann hypothesis*; M. O. Rabin modified it to obtain an unconditional probabilistic algorithm.

The Miller–Rabin primality test is based on the following statement:

- *For a given odd number n, for which $n-1 = 2^k \cdot d$, if we can find an a such that*

  $$a^d \not\equiv 1 (mod\ n), \quad and \quad a^{2^r d} \not\equiv -1 (mod\ n) \quad for\ all \quad r \in [0, n-1],$$

  then n is composite.

In this case a is called a *strong witness* for the compositeness of n.

Otherwise, n can be prime, but can also be composite. If n is a composite number such that

$$a^d \equiv 1 (mod\ n), \quad \text{or} \quad a^{2^r d} \equiv -1 (mod\ n) \quad \text{for some} \quad r \in [0, n-1],$$

the base a is called a *strong liar*, and n is a *strong probable prime* to base a.

The smallest odd composite strong probable primes (SPRPs) are the following:

- $2047 = 23 \cdot 89$ is a 2-SPRP;
- $121 = 11 \cdot 11$ is a 3-SPRP;
- $781 = 11 \cdot 71$ is a 5-SPRP;
- $25 = 5 \cdot 5$ is a 7-SPRP.

For every odd composite n, there are many witnesses a. In fact, for a given composite number n, at least $\frac{3}{4}$ of numbers $a \in [2, n-1]$ are witnesses of compositeness of n. However, no simple way of generating such an a is known. The solution is to make the test probabilistic: We choose a randomly and check whether or not it is a witness for the compositeness of n. If n is composite, most of the numbers a are witnesses; thus, the test will detect n as composite with high probability: The test declares a composite n as probably prime with a probability at most 4^{-k}, where k is the number of different values of a we test.

2.5.8. However, there exist several classical *criterions of primality* of a given positive integer n.

A well-known criterion of primality is given by the *Wilson's theorem* (also known as *Al-Haytham's theorem*).

Theorem (Wilson's theorem). *A positive integer p is a prime number if and only if*

$$(p-1)! \equiv -1 (mod\ p).$$

□ The simplest proof uses the fact that if p is an odd prime, then the set of residue classes $Z/pZ^* = \{[1]_p, [2]_p, \ldots, [p-1]_p\}$ forms a group under multiplication modulo p.

This means that for each element $[a]_p \in Z/pZ^*$, there is a unique inverse element $[b]_p \in Z/pZ^*$ such that $a\dot{b} \equiv 1 (mod\ p)$.

If $a \equiv b (mod\ p)$, then $a^2 \equiv 1 (mod\ p)$, which forces

$$a^2 - 1 = (a+1)(a-1) \equiv 0 (mod\ p),$$

and since p is prime, this forces

$$a \equiv 1, \quad \text{or} \quad a \equiv -1 (mod\ p),$$

i.e., $a = [1]_p$ or $a = [p-1]_p$.

In other words, $[1]_p$ and $[p-1]_p$ are each their own inverse, but every other element has a distinct inverse, and so, if we collect the elements from Z/pZ^* pairwise in this fashion and multiply them all together, we get the product -1.

For example, if $p = 11$, we have

$$10! \equiv (1 \cdot 10)(2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(6 \cdot 8) \equiv -1 (mod\ 11).$$

If $p = 2$, the result is trivial to check.

For a converse, suppose the congruence

$$(n-1)! \equiv -1 (mod\ n)$$

holds for a composite n, and note that then n has a proper divisor d with $1 < d < n$.

Clearly, d divides $(n-1)!$. But by the congruence above, d also divides $(n-1)! + 1$ so that d divides 1, a contradiction. □

Unfortunately, Wilson's theorem is useless as a primality test since computing $(n-1)!$ is difficult for large n.

The following criterion of primality for a given positive integer n is more effective:

- *A positive integer $n > 2$ is a prime number if and only if there exists some positive integer a, $1 < a < n$, such that*

$$a^{n-1} \equiv 1 (mod\ n), \quad \text{and} \quad a^{\gamma} \not\equiv 1 (mod\ n)$$

$$\text{for all positive integers } \gamma | (n-1).$$

□ In fact, by multiplicative order's properties, we obtain from the condition $a^{n-1} \equiv 1 (mod\ n)$, that $ord_n\, a | (n-1)$, and from the second condition, it follows that $ord_n\, a = n-1$. As $ord_n\, a | \phi(n)$, then $n - 1 | \phi(n)$; as $\phi(n) < n$ for $n \neq 1$, then $\phi(n) = n-1$, i.e., $n \in P$.

Conversely, if n is a prime number, then there exists a primitive root g modulo n. It is a generator of the group Z/nZ^*. Such a generator has order $|Z/nZ^*| = n-1$ and both equivalences will hold for any such primitive root:

$$g^{n-1} \equiv 1 (mod\ n) \ \text{ and } \ g^{\gamma} \not\equiv 1 (mod\ n)$$
$$\text{for all positive integers } \gamma|(n-1). \qquad \square$$

Of course, there is no need to check all positive integer exponents $\gamma|(n-1)$. It is enough to check only γ of the form $\frac{n-1}{q}$ for all prime divisors of n. So, we get the following criterion of primality:

- *A positive integer $n > 2$ is a prime number if and only if there exists some positive integer a, $1 < a < n$, such that*
$$a^{n-1} \equiv 1 (mod\ n), \ \text{ and } \ a^{\frac{n-1}{q}} \not\equiv 1 (mod\ n)$$
$$\text{for any prime factor } \ q \ \text{ of } \ n.$$

This result was obtained by the French mathematician François Édouard Anatole Lucas (1842–1891). In computational number theory, the corresponding test is called the *Lucas test*.

It is a deterministic primality test which can be applied to any positive integer $n > 2$. However, it requires that all prime factors of $n - 1$ to be known.

Formulas of primes

A *formula for primes* is a formula generating the prime numbers exactly and without exception. No such formula is known.

2.5.9. It was proven (Goldbach, 1752) that

- *no non-constant polynomial $f(x)$ with integer coefficients can give a prime for all integers values of x.*

Legendre showed that

- *there is no rational algebraic function which always gives primes.*

Using more algebraic number theory, one can show an even stronger result:

- *No non-constant polynomial $f(n)$ exists that evaluates to a prime number for almost all integers n.*

However, there exist polynomials which can give many prime numbers. So, the *Euler polynomial* (Euler, 1772) $f(x) = x^2 + x + 41$ gives a prime for all non-negative integers less than 40. For $n = 40$, it produces a square number, 1681, which is equal to 41^2, the smallest composite number for this formula.

The quadratic polynomial $x^2 - x + 41$ (Legendre, 1798) gives the same prime numbers for $x = 1, \ldots, 40$, and gives composite numbers for 41 and 42.

The polynomial $g(x) = x^2 - 79x + 1601$ gives primes for $x = 0, \ldots, 79$, corresponding to the 40 primes given by the above formula taken twice each.

It is known, based on *Dirichlet's theorem on the existence of primes in a given arithmetic progression* (Dirichlet, 1837), that

- *the linear polynomial function $f(x) = ax + b$ produces infinitely many primes as long as a and b are relatively prime.*

In particular, there are infinitely many primes of the form $4x - 1$, $4x + 1$, $6x - 1$, and $6x + 1$.

It is not known, however, whether there exists a polynomial of degree greater than one that assumes an infinite number of values that are prime. In particular, it is not known whether there are infinitely many primes of the form $ax^2 + bx + c$ and, especially, of the form $x^2 + 1$.

2.5.10. After the simplest algebraic function, a polynomial, it is natural to consider the exponential function, $f(n) = k^n$ or, as the value k^n cannot give infinitely many primes, the variant of it of the form

$$f(n) = k^n \pm b^n.$$

As for any positive integer n, one has

$$k^n - b^n = (k - b)(k^{n-1} + k^{n-2}b + \cdots + k^2b^{n-2} + b^{n-1}),$$

then $k^n - b^n$ can be prime only in the case $k - b = 1$ or $k = b + 1$. In the simplest case, we have $b = 1$, i.e.,

$$f(n) = k^n - 1.$$

The same choice of b gives us in the case $k^n + b^n$ the function

$$f(n) = k^n + 1.$$

For $k^m + 1$ to be prime, k must be even and the exponent m must be a power of 2. The simplest case $k = 2$ gives us the *Fermat numbers*:

$$F_n = 2^{2^n} + 1,\ n = 0, 1, 2, 3, \ldots .$$

If $k^m - 1$ is a prime, then $k = 2$ and m is a prime, so the problem is reduced to that of *Mersenne numbers*:

$$M_p = 2^p - 1,\ p \in P.$$

Fermat numbers

2.5.11. The *Fermat numbers* $F_n = 2^{2^n} + 1,\ n = 0, 1, 2, 3, \ldots$ were studied by the 17th century French mathematician Pierre Fermat (1607–1665), who conjectured (1640) that they would always give a prime for $n = 0, 1, \ldots$. The first five Fermat numbers are primes: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$ (see sequences A019434 and A000215 in the OEIS). But in 1732, Euler found that F_5 is a composite number:

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417.$$

□ To show it, consider $2^{32} + 1 = 2^4 \cdot 2^{28} + 1$ and write $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$. Therefore, $5^4 \equiv -2^4 (mod\, 641)$, and $5 \cdot 2^7 \equiv -1 (mod\, 641)$. Then, we obtain that $5^4 \cdot 2^{28} \equiv 1 (mod\, 641)$, or $-2^4 \cdot 2^{28} \equiv 1 (mod\, 641)$, or $2^{32} + 1 \equiv 0 (mod\, 641)$. □

So, Fermat's conjecture that F_n is always prime is clearly false. Beyond F_4, no further Fermat primes have been found. In fact, F_n is a composite number for all n from 5 to 32 and for many higher values of n, although for some composite Fermat numbers, not all the factors are known.

In general, as of 2021, more than 300 Fermat numbers are known to be composite. The largest known composite Fermat number (proper, Reynolds, Penné, and Fougeron, 2020) is $F_{18233954}$; it has the prime factor $p = 7 \cdot 2^{18233956} + 1$.

The Fermat numbers have an interesting connection with the classical problem of constructing a regular polygon by Euclidean methods, i.e., by the use of an unmarked ruler and a compass. In 1796, Gauss, at the age of 19, proved that

- *a regular n-gon can be constructed by Euclidean methods if and only if*

  $$n = 2^r p_1 \cdot \ldots \cdot p_k,$$

  where p_i are distinct Fermat primes, i.e., n is a power of two times a product of distinct Fermat primes.

Open questions

1. Are there infinitely many composite Fermat numbers?
2. Are there infinitely many Fermat primes?
3. Is there at least one Fermat prime $> F_4$?

Mersenne numbers

2.5.12. *Mersenne numbers* are integers of the form $M_n = 2^n - 1$ (many authors require that the exponent n be a prime). The first few Mersenne numbers are 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, 16383, 32767, ... (sequence A000225 in he OEIS).

They are of interest because the Mersenne primes (prime Mersenne numbers) are among the oldest and most studied of all primes.

Although numbers of the form $2^n - 1$ had been investigated before the 17th century, they are named after Martin Mersenne (1588–1648), a French monk and mathematician, because he discussed them in his work *Cogita Physico Mathematics* and stated conjectures about the number's occurrence. One of his most famous conjectures was that $2^n - 1$ is prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ and is composite for all other integers $2 \leq n \leq 257$.

It is obvious that Mersenne could not have tested all of these numbers. It took three centuries and several mathematical discoveries (such as the Lucas–Lehmer test), before the exponents in Mersenne's conjecture had been completely checked. It was determined that he had made five errors (three primes omitted, two composites listed), and the correct list is: $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$, and 127.

So, the *Mersenne conjecture* was not completely correct, but his name is still attached to the numbers.

The Mersenne numbers give us most of prime number records. For example, in 1999 (Hajratwala, Woltman, Kurowski *et al.*), the first prime with more than 1000000 decimal digits (in fact, more than 2000000) was obtained. It is the 38th Mersenne prime, $M_{6972593}$; it has 2098960 decimal digits. In 2018 (Laroche, Woltman, Blosser *et al.*), the last known (in fact, the 51st known) Mersenne prime, $M_{82589933}$, was obtained. It has 24862048 decimal digits.

Similar to Fermat numbers, Mersenne numbers are connected to a very old mathematical problem. Due to the *Euclid–Euler theorem*, any even perfect number has the form

$$n = 2^{p-1}(2^p - 1),$$

where $2^p - 1$ is a Mersenne prime. So, we obtain new perfect number if and only if we obtain a new Mersenne prime. As for odd perfect numbers, mathematicians cannot find one. If odd perfect numbers exist, they should be very large and very special.

Conjectures and unsolved problems

1. Are there infinitely many Mersenne primes? (Equivalently, we could ask: Are there infinitely many even perfect numbers?)
2. Are there infinitely many Mersenne composites (i.e., composite numbers $M_p = 2^p - 1$ with prime index p)?
3. Is every Mersenne number M_p square-free?

We consider these and other questions in Chapter 3.

Prime number theorem

2.5.13. As we studied in the previous sections, there are no good candidates to arithmetic functions which can be used as formulas of primes.

Moreover, the irregularity of the distribution of prime numbers on the number line is well known. On the one hand,

- *for a given N, there exists an interval of length N which does not contain prime numbers.*

□ In fact, the number $(N+1)!+2$ is divisible by 2, $(N+2)!+3$ is divisible by 3,…, $(N+1)!+(N+1)$ is divisible by $(N+1)$. □

On the other hand, there exist the so-called *twin primes*: If you look down the list of primes, you will quite often see two consecutive odd numbers: 3 and 5, 5 and 7, 11 and 13, 17 and 19,…. We call these pairs of prime numbers, $\{p, p+2\}$, *twin primes*. This name was coined by Stackel in 1916. The first such pairs are: (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139), (149, 151), (179, 181), (191, 193), (197, 199), …(sequence A077800 in the OEIS).

A question to which the answer is not known is

- *whether there exist infinitely many twin primes,*

though it has been proved by Brun in 1919 that the series of the reciprocals of the prime numbers of the pairs of twin primes is finite or convergent.

For all these reasons, the best arithmetic function, which is used for the study of distribution of prime numbers, is *prime counting function*.

2.5.14. For any positive real number x, let the *prime counting function* $\pi(x)$ be the number of primes not greater than x:

$$\pi(x) = \sum_{p \leq x} 1.$$

We have $\pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = \pi(4) = 2$, $\pi(5) = \pi(6) = 3$, …, $\pi(100) = 25$, $\pi(1000) = 168$, $\pi(10000) = 1229$, $\pi(10^5) = 9592$, $\pi(10^6) = 78498$, $\pi(10^7) = 664579$, $\pi(10^8) = 5761455$, and $\pi(10^9) = 50847534$ (see sequence A006880 in the OEIS).

In 1972, Bohman calculated that $\pi(10^{10}) = 455052511$. Lagarias, Miller, and Oleyzko have computed the value $\pi(10^{16}) = 279238341033925$.

At present, we know that $\pi(10^{28}) = 157589269275973410412739598$ (Baugh and Walisch, 2020).

Obviously, we have that $\pi(p_n) = n$.

From the Euclid's theorem, it follows that

$$\pi(x) \to \infty \quad \text{as} \quad x \to \infty.$$

Another proof of Euclid theorem was given by Euler in 1737. He considered the series

$$1 + \frac{1}{2^s} + \cdots + \frac{1}{n^s} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

for $s \in \mathbb{R}, s > 1$. He evaluated the sums $\zeta(2k)$ for every $k \geq 1$; in particular, the values $\zeta(2) = \frac{\pi^2}{6}$ and $\zeta(4) = \frac{\pi^4}{90}$ were obtained.

Euler noticed that

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in P} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots\right) = \prod_{p \in P} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Due to this observation, he gave an analytic proof of the infiniteness of prime numbers.

In fact, he proved that

- *the sum* $\sum_{p \in P} \frac{1}{p}$ *of the inverses of the prime numbers is divergent:*

$$\sum \frac{1}{p} = \log \log x + O(1).$$

Euler also proved that

$$\pi(x) = o(x), \text{ i.e., } \lim_{x \to \infty} \frac{\pi(x)}{x} = 0.$$

2.5.15. In 1792, Gauss had conjectured that there exists such an asymptotic formula for the function $\pi(x)$:

$$\pi(x) \sim \frac{x}{\log x}, \quad \text{as} \quad x \to \infty.$$

Later, he refined this estimate to

$$\pi(x) \sim \int_2^x \frac{du}{\log u}.$$

Gauss did not publish this result, which he first mentioned in 1849 (in a letter to Encke). It was subsequently posthumously published in 1863.

Legendre, 1808, conjectured a similar result:

$$\pi(x) \sim \frac{x}{\log x - 1.08366}.$$

2.5.16. The first essential success in this problem was achieved by Chebyshev in 1850. He found the following boundaries for the function $\pi(x)$:

$$a \cdot \frac{x}{\log x} < \pi(x) < b\frac{x}{\log x},$$

where $x \geq 2$, $a = \frac{2^{1/2}3^{1/3}5^{1/5}}{30^{1/30}}$, and $b = \frac{6}{5}a$; hence, the new boundaries for the nth prime number p_n were found:

$$0.91 \cdot n \log n < p_n < 1.7 \cdot n \log n.$$

Chebyshev also proved the well-known *Bertrand's postulate*:

- *If n is a natural number > 1, then between n and $2n$, there is at least one prime number.*

2.5.17. The fundamental contribution to further investigations on the problem of distribution of primes was made by Riemann in 1859. He returned to Euler's proof of infiniteness of primes and introduced the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \cdots + \frac{1}{n^s} \cdots$$

as a function of a complex variable $s = \sigma + it$, $\sigma > 1$. This sum absolutely convergent for *Re* $s = \sigma > 1$ and represents an analytic function in this region. Riemann showed that $\zeta(s)$ is analytically continuable on the whole complex plane and has a simple pole with the residue 1 at the point $s = 1$.

Moreover, Riemann showed that the zeta function satisfies a functional equation from which it follows that it has zeros at

$$s = -2, -4, \ldots, -2n, \ldots$$

(the so-called *trivial zeros*) and that all other zeros lie in the strip $0 \leq$ *Re* $s \leq 1$, the so-called *critical strip*. The *Riemann hypothesis* asserts that

- *all the non-trivial zeros of the zeta function actually lie on the critical line Re* $s = \frac{1}{2}$.

The conjecture currently remains unproven. Numerical computations have been made to check the Riemann hypothesis for the first $1.2 \cdot 10^{13}$ zeros.

2.5.18. Riemann first realized the connection between the distribution of primes and the distribution of the non-trivial zeros of the zeta function. Further progress led to the proving of the *prime number theorem* in 1896, independently by Hadamard and de la Vallée Poussin.

Theorem (prime number theorem). *It holds that*

$$\pi(x) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right), \quad \text{i.e.,} \quad \lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

The main part of the proof was establishing that $\zeta(1+it) \neq 1$ for any $t \in \mathbb{R}$.

More exactly, Vallée Poussin (1899) showed that for some constant a it holds that

$$\pi(x) = Li(x) + O\left(\frac{x}{\log x} e^{-a\sqrt{\log x}}\right).$$

In 1901, Koch showed that if the Riemann hypothesis is true, then

$$\pi(x) = Li(x) + O(\sqrt{x}\log x),$$

which can be written in the slightly weaker form

$$\pi(x) = Li(x) + O(x^{1/2+\epsilon}).$$

So, from the Riemann hypothesis, we can obtain a good estimation for $\pi(x)$ with an error term of the order $\sqrt{x}$. The best bounds known today are far from this result.

As a consequence of the prime number theorem, one gets an asymptotic expression for the nth prime number:

$$p_n \sim n \log n.$$

A better approximation is

$$p_n = n\log n + n\log\log n + O\left(\frac{n}{\log n}\log\log n\right).$$

2.5.19. The *Riemann zeta function* $\zeta(s)$ is defined for any complex number $s = \sigma + it$ with real part $\sigma > 1$ by the following Dirichlet series:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

It is well known that

- *in the region Re* $s > 1$, *the infinite series* $\sum_{n=1}^{\infty} \frac{1}{n^s}$ *converges and defines an analytic function.*

☐ We know that $e^{i\phi} = \cos\phi + i\sin\phi$, i.e., $|e^{i\phi}| = \sqrt{\cos^2\phi + \sin^2\phi} = 1$. Then,

$$\left|\frac{1}{n^s}\right| = \left|\frac{1}{n^\sigma} e^{it\log n}\right| = \frac{1}{n^\sigma}.$$

As the series $\sum_{n=1}^{\infty} \frac{1}{n^\sigma}$ is convergent for $\sigma > 1$, then the series $\sum_{n=1}^{\infty} \frac{1}{n^s}$ is uniformly convergent in any domain $\sigma > 1 + \delta$, $\delta > 0$; hence, in this domain, the sum of the series is an analytic function. As δ is any positive number, the last proposition is true in the domain $\sigma > 1$. ☐

Using this fact, we can show that

- *for Re* $s = \sigma > 1$, *one has*

$$\zeta'(s) = -\sum_{n=2}^{\infty} \frac{\log n}{n^s}.$$

☐ In fact,

$$\zeta'(s) = \sum_{n=1}^{\infty} (n^{-s})' = \sum_{n=1}^{\infty} (-n^{-s})\log n = -\sum_{n=2}^{\infty} \frac{\log n}{n^s}. \qquad \square$$

The connection between zeta function and prime numbers was already realized by Euler: He proved (for real $s > 1$) that

$$\zeta(s) = \prod_{p\in P} \frac{1}{1 - p^{-s}},$$

where we have an infinite product extending over all prime numbers p. This equality is called the *Euler product formula*. It converges for $Re\ s > 1$. It is a consequence of two simple and fundamental results in mathematics: the formula for the geometric series and the fundamental theorem of arithmetic.

□ Each factor (for a given prime p) in the product above can be expanded to a geometric series consisting of the reciprocal of p raised to multiples of s, as follows:

$$\frac{1}{1-p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots .$$

When $Re\ s > 1$, this series converges absolutely. Hence, we may take a finite number of factors, multiply them together, and rearrange terms:

$$\begin{aligned}\prod_{p\le X}(1-p^{-s})^{-1} &= \prod_{p\le X}(1+p^{-s}+p^{-2s}+\cdots)\\ &= \sum^{*}\frac{1}{n^s} = \sum_{n\le X}\frac{1}{n^s} + \sum_{n>X}^{\prime\prime}\frac{1}{n^s}.\end{aligned}$$

(By the fundamental theorem of arithmetic, the partial product when expanded out gives a sum $\sum^*$ consisting of those terms $\frac{1}{n^s}$, where n is a product of primes less than or equal to X.)

As $X \to \infty$ and $\sum_{n=1}^{\infty}\frac{1}{n^s}$ is absolutely convergent, then $\sum_{n>X}\frac{1}{n^s} \to 0$ and $\sum''\frac{1}{n^s} \to 0$, so the above formula holds. □

The following sketch of an another proof only makes use of simple algebra that most high-school students can understand. In fact, this was originally the method by which Euler discovered the formula. There is a certain sieving property that we can use to our advantage:

$$\zeta(s) = 1 + \frac{1}{2^s} + \cdots \quad\text{and}\quad \frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \cdots .$$

By subtracting the second from the first, we remove all elements that have a factor of 2:

$$\left(1-\frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \cdots .$$

Repeating for the next term,

$$\frac{1}{3^s}\left(1-\frac{1}{2^s}\right)\zeta(s)=\frac{1}{3^s}+\frac{1}{9^s}+\cdots,$$

and subtracting again, we get

$$\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s)=\frac{1}{5^s}+\frac{1}{7^s}+\frac{1}{11^s}+\cdots.$$

It can be seen that the right-hand side is being sieved. Repeating infinitely, we get

$$\ldots\left(1-\frac{1}{11^s}\right)\ldots\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s)=1.$$

Dividing both sides by everything but $\zeta(s)$, we obtain

$$\zeta(s)=\frac{1}{(1-\frac{1}{2^s})(1-\frac{1}{3^s})\ldots(1-\frac{1}{11^s})\ldots}.$$

This can be written more concisely as an infinite product over all primes p.

To make this proof rigorous, we need only observe that when $Re\ s > 1$, the sieved right-hand side approaches 1, which follows immediately from the convergence of the Dirichlet series for $\zeta(s)$. □

The Euler result is a particular case of a general formula of such kind:

- *Let f be completely multiplicative function, and $\sum_{n=1}^{\infty} f(n)$ is absolutely convergent for $Re\ s > 1$; then,*

$$\sum_{n=1}^{\infty} f(n)=\prod_{p}(1-f(p))^{-1}.$$

The following are values of the zeta function for the first few natural numbers:

- $\zeta(1)=\infty$; this is the harmonic series;
- $\zeta(2)=\frac{\pi}{6}=1.645\ldots$ (the demonstration of this equality is known as the *Basel problem*);
- $\zeta(3)=1.202\ldots$ (this is called *Apéry's constant*);
- $\zeta(4)=\frac{\pi^2}{90}=1.0823\ldots.$

2.5.20. Consider now the *von Mangoldt function* — an arithmetic function named after the German mathematician Hans Carl Friedrich von Mangoldt (1854–1925).

The *von Mangoldt function* $\Lambda(n)$ is defined as $\Lambda(n) = \log p$ if $n = p^k$ for prime p and positive integer k and $\Lambda(n) = 0$ otherwise.

It is an example of an important arithmetic function that is neither multiplicative nor additive.

It is easy to show that

- *the von Mangoldt function satisfies the identity*

$$\log n = \sum_{d|n} \Lambda(n).$$

□ In fact, for $n = 1$, we have the identity $0 = \log 1$. For $n \neq 1$, we obtain

$$\sum_{d|n} \Lambda(d) = \log p_1^{\alpha_1} \dots p_k^{\alpha_k} = \log n. \qquad \square$$

The summatory von Mangoldt function, $\psi(x)$, known as the *Chebyshev function*, is defined as

$$\psi(x) = \sum_{n \leq x} \Lambda(n).$$

The von Mangoldt function plays an important role in the theory of Dirichlet series and, in particular, the Riemann zeta function. It is easy to prove that

- *for Re $s > 1$, one has*

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

□ Really, it holds that $\log \zeta(s) = \sum_p \log(1 - p^{-s})^{-1}$; therefore,

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_p \frac{p^{-s}\log p}{1 - p^{-s}} = -\sum_p \sum_{k=1}^{\infty} \frac{\log p}{p^{ks}} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

The formula is proved. □

There are a number of similar relations involving various well-known multiplicative functions.

So, *the reciprocal of the zeta function may be expressed as a Dirichlet series over the Möbius function*:

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}, \mathit{Re}\ s > 1.$$

The second degree of the zeta function is connected with the divisor function $\tau(n) = \sum_{d|n} 1$:

$$\zeta^2(s) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s},\ \mathit{Re}\ s > 1.$$

□ In fact, $\zeta^2(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{m=1}^{\infty} \frac{1}{m^s} = \sum\sum_{n,m=1}^{\infty} \frac{1}{(nm)^s} = \sum_{k=1}^{\infty} \frac{\tau(k)}{k^s}$, where $k = nm$. □

In general,

$$\zeta^k(s) = \sum_{n=1}^{\infty} \frac{\tau_k(n)}{n^s},\ \mathit{Re}\ s > 1,$$

where $\tau_k(n) = \sum_{n=n_1\ldots n_k} 1$ is the number of representations of a given positive integer n as a product of k positive integers.

For the proof of the prime number theorem, it is important to use the following fact about a similar behavior of the prime counting function $\pi(x)$ and the Chebyshev function $\psi(x)$. It is not so difficult to show that

- *the three following propositions are equivalent*:
  1. $\pi(x) = \frac{x}{\log x} + o(\frac{x}{\log x})$, *where* $\pi(x) = \sum_{p\leq x} 1$;
  2. $\psi(x) = x + o(x)$, *where* $\psi(x) = \sum_{n\leq x} \Lambda(n) = \sum_{p^k\leq x} \log p$;
  3. $\omega(x) = x + o(x)$, *where* $\omega(x) = \int_1^x \frac{\psi(t)}{t} dt = \sum_{n\leq x} \Lambda(n) \log \frac{x}{n}$.

Dirichlet's characters and *L*-functions

2.5.21. *Dirichlet characters* are certain arithmetic functions that capture some important properties of the cyclic group. They are named in honor of a German mathematician Johann Peter Gustav Lejeune Dirichlet (1805–1859).

A complex-valued arithmetic function $\chi : \mathbb{Z} \to \mathbb{C}$ is called a *Dirichlet character modulo* n, where n is a positive integer if for all integers a and b it holds that

- $\chi(a) = \chi(a+n)$;
- $\chi(a) = 0$ for every a with $gcd(a,n) > 1$;
- $\chi(ab) = \chi(a)\chi(b)$;
- $\chi(1) = 1$.

Condition 1 says that the character is periodic with period n. Conditions 3 and 4 say that characters are completely multiplicative.

The *principal character* modulo n, denoted by χ_0, is defined as $\chi_0(a) = 1$ if $gcd(a,n) = 1$ and as $\chi_0(a) = 0$ if $gcd(a,n) > 1$.

Properties of Dirichlet characters

1. The number of characters modulo n is $\phi(n)$.
2. $\chi(a)$ is an $\phi(n)$-root from the unity.
3. $|\chi(a)| \leq 1$.
4. $\sum_{\chi} \chi(a) = \phi(n)$ if $a \equiv 1(modn)$, and $= 0$ otherwise.
5. $\sum_{o \leq a < m} \chi(a) = \phi(n)$ if $\chi = \chi_0$ and $= 0$ otherwise.
6. $|\sum_{a \leq x} \chi(a)| \leq n$ for $\chi \neq \chi_0$.

2.5.22. Dirichlet characters are used to define *Dirichlet L-functions*, which are meromorphic functions with a variety of interesting analytic properties.

For a given n and a given Dirichlet character $\chi(n)$ modulo n, the *Dirichlet L-function* $L(s,\chi)$ is defined for *Re* $s > 1$ as the following Dirichlet series:

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

It is easy to show that the L-functions have many properties similar to the properties of the Riemann zeta function. In fact, $\zeta(s) = L(s,\chi_0)$, where χ_0 is the only character which is modulo 1, i.e., $\chi_0(a) = 1$ for any positive integer a.

Properties of L-functions

1. For $Re\ s > 1$, one has $L(s,\chi) = \prod_p (1 - \frac{\chi(p)}{p^s})^{-1}$.
2. For $Re\ s > 1$, one has $-L'(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n^s}$.
3. For $Re\ s > 1$, one has $-\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n-1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s}$.
4. $L(s,\chi_0) = \zeta(s)\prod_{p|n}(1 - \frac{1}{p^s})$.

Dirichlet characters and their L-series were introduced by Dirichlet in 1831 in order to prove *Dirichlet's theorem about the infinitude of primes in arithmetic progressions.* He only studied them for real s and especially as s tends to 1. The extension of these functions to complex s in the whole complex plane was obtained by Bernhard Riemann in 1859.

Proof of the Dirichlet's theorem for the simplest cases

2.5.23. In this section, we consider the proof of the *Dirichlet's theorem on primes in arithmetic progressions* for the simplest arithmetic progressions $4x + 1$ and $4x - 1$.

We use the fact that for $n = 4$, there are exactly two characters: $\chi_0(n) = 1$ for odd n and $\chi_0(n) = 0$ otherwise; $\chi_1(n) = 1$ for $n \equiv 1 (mod\ 4)$, $\chi_1(n) = -1$ for $n \equiv -1 (mod\ 4)$, and $\chi_1(n) = 0$ otherwise.

Theorem (Dirichlet's theorem on primes in the arithmetic progressions $4x \pm 1$). *The sets of primes of the forms $4k - 1$ and $4k + 1$ are infinite.*

□ **I.** Elementary proof

For the case of the numbers of the form $4k - 1$, we can apply the Euclidean method. In fact, any number of the form $4k - 1$ has a prime divisor of the same form: such a number $\neq 1$ and is an odd number and, hence, has a prime divisor which cannot be 2, so should be of the form $4k - 1$ or of the form $4k + 1$. If all prime divisors of n are of the form $4k + 1$, then n should be of the form $4k + 1$, a contradiction.

Suppose that the set of primes of the form $4k-1$ is finite and that $p_1, \dots, p_k$ are all such primes.

Consider

$$E = 4p_1 \dots p_k - 1.$$

This number has the form $4m-1$ and, hence, has the prime divisor p of the same form. Then, $p = p_i$ for some p_i and, therefore, $p|p_1 \dots p_k$, i.e., $p|1$, a contradiction.

For the prime numbers of the form $4k+1$, the Euclidean method does not work, as some numbers of the form $4k+1$ have only prime divisors of the form $4k-1$, for example, the number 25. In this case, suppose that the set of the primes of the form $4k+1$ is finite and that $q_1, \dots, q_s$ are all such primes.

Consider

$$E = 4(q_1, \dots, q_k)^2 + 1.$$

Let $p|E$. Then, $p \neq 2$ and $(2q_1, \dots, q_s)^2 \equiv -1(mod\ p)$, i.e., -1 is a quadratic residue modulo p; therefore, $p \equiv 1(mod\ 4)$. Then, $p = q_i$ for some $i = 1, \dots, s$, and $p|q_1 \dots q_s$, i.e., $p|1$, a contradiction.

II. Analytic proof

Consider the functions $L_i(s) = \sum_{n=1}^{\infty} \frac{\chi_i(n)}{n^s}$, for $i = 0$ and 1, i.e.,

$$L_0(s) = \sum_{k=0}^{\infty} \frac{1}{(2k+1)^s}, \quad \text{and} \quad L_1(s) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)^s}.$$

It is easy to see that both series are absolutely convergent for $Re\ s > 1$, and the second is convergent for $Re\ s > 0$.

Moreover,

$$L_1(1) = 1 - \frac{1}{3} + \frac{1}{5} \cdots > 1 - \frac{1}{3} = \frac{2}{3},$$

i.e., $L_1(1) = const \neq 0$.

On the other hand,

$$L_0(s) \geq \frac{1}{2} \int_0^{\infty} \frac{d(2x+1)}{(2x+1)^s} = \frac{1}{2} \frac{(2x+1)^{1-s}}{1-s} |_0^{\infty} = \frac{1}{2(s-1)},$$

and $\frac{1}{2(s-1)} \to \infty$ as $s \to 1+$, i.e., $L_0(s) \to \infty$ as $s \to 1+$. As

$$\sum_{n=1}^{\infty} \frac{\chi_i(n)}{n^s} = \prod_p (1 - \frac{\chi_i(p)}{p^s})^{-1},$$

then

$$\log L_i(s) = -\sum_p \log(1 - \frac{\chi(p)}{p^s}) = \sum_p \sum_{k=1}^{\infty} \frac{(\chi(p))^k}{kp^{ks}},$$

and

$$-\frac{L_i'(s)}{L_i(s)} = \sum_{n=2}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s}.$$

Therefore,

$$-\frac{L_i'(s)}{L_i(s)} = \sum_p \frac{\log p\chi(p^k)}{p^{ks}} = \sum_p \frac{\log p\chi(p)}{p^s} + \sum_p \sum_{k=2}^{\infty} \frac{\log p\chi(p^k)}{p^{ks}}.$$

For the absolute value of the second sum (for all $k \geq 2$), it holds that

$$\begin{aligned} \sum_p \sum_{k=2}^{\infty} \frac{\log p\chi(p^k)}{p^{ks}} &\leq \sum_p \sum_{k=2}^{\infty} \frac{\log p}{p^{k\sigma}} = \sum_p \log p \left(\frac{1}{p^{2\sigma}} + \frac{1}{p^{3\sigma}} + \cdots \right) \\ &= \sum_p \log p \frac{p^{-2\sigma}}{1 - p^{-\sigma}} \leq 2 \sum_p \log p \frac{1}{p^{2\sigma}} = O(1). \end{aligned}$$

Therefore,

$$\sum_p \log p \frac{\chi_i(p)}{p^s} = \frac{L_i'(s)}{L_i(s)} + O(1),$$

or

$$\sum_{p \equiv 1 (mod\ 4)} \frac{\log p}{p^s} + \sum_{p \equiv -1 (mod\ 4)} \frac{\log p}{p^s} = \frac{L_0'(s)}{L_0(s)} + O(1),$$

and

$$\sum_{p \equiv 1 (mod\ 4)} \frac{\log p}{p^s} - \sum_{p \equiv -1 (mod\ 4)} \frac{\log p}{p^s} = \frac{L_1'(s)}{L_1(s)} + O(1).$$

Therefore, we obtain that

$$\sum_{p\equiv 1(mod\ 4)} \frac{\log p}{p^s} = \frac{1}{2}\left(\frac{L_0'(s)}{L_0(s)} + \frac{L_1'(s)}{L_1(s)}\right) + O(1), \quad \text{and}$$

$$\sum_{p\equiv 3(mod\ 4)} \frac{\log p}{p^s} = \frac{1}{2}\left(\frac{L_0'(s)}{L_0(s)} - \frac{L_1'(s)}{L_1(s)}\right) + O(1).$$

As $L_1(s) = O(1)$ for $s \to 1+$, and $L_1(s) \to \infty$ for $s \to 1+$, then the right-hand parts of both equalities above $\to \infty$ for $s \to 1+$, and both series, $\sum_{p\equiv 1(mod\ 4)} \frac{\log p}{p}$ and $\sum_{p\equiv -1(mod\ 4)} \frac{\log p}{p}$, are divergent, i.e., there are infinitely many primes of the form $4k+1$, and there are infinitely many primes of the form $4k-1$. □

For the full proofs of all properties and theorems, as well as many examples and some additional information, see, for example, in [Apos86], [Dave47], [Buch09], [DeDe12], [DeKo13], [Deza17], [Deza21], [Deza18], [Dick05], [Eule48], [HaWr79], [Hool76], [Ingh32], [Ivic85], [Kara83], [Lagr70], [Luca75], [Sier64], and [Wiki22]. See also references to Chapter 2 in [Deza21].

Exercises

1. Prove that any composite number n has a prime divisor $p \le \sqrt{n}$.
2. Prove that for a given $n \ge 3$ between n and $n!$, there exists at least one prime number; prove that there exist infinitely many prime numbers.
3. Prove that there are infinitely many primes of the form $6k-1$.
4. Prove the following fact: If p is a prime number, and $p-1 = 2^k d$, where d is an odd number, then for every a coprime with p, it holds that $a^d \equiv 1(modp)$ or $a^{2^r d} \equiv -1(modp)$ for some $r \in [0, \dots, k-1]$. (See Rabin–Miller strong pseudoprime test.)
5. Prove that there are infinitely many primes of the form $x^2 - y^2$.
6. Prove that $(F_n, F_m) = 1$; $F_n \ne p+q$; and $F_n | F_{n+k} - 2$.
7. Prove that $M_n | M_{nm}$; $M_{n-m} | M_n - M_m$; and $gcd(M_n, M_m) = M_{gcd(n,m)}$.
8. Prove that for a given prime p, the Legendre symbol $(\frac{a}{p})$ is a Dirichlet character.

9. Construct all Dirichlet characters modulo 4, modulo 5, and modulo 6. Construct all Dirichlet L-functions modulo 4, modulo 5, and modulo 6. Prove the Diriclet's theorem for the progressions $5x \pm 1$ and $6x \pm 1$.

2.6. Divisor Functions

Basic notions

2.6.1. A *divisor* of an integer n is an integer m that may be multiplied by some integer to produce n, i.e., there exists an integer k such that $n = k \cdot m$.

In this case, one also says that n is divisible by m, n is a multiple of m, and m is a factor of n. This is written as $m|n$. If m does not divide n, then the notation is $m \not| n$.

1 and -1 divide (or are divisors of) every integer. Every non-zero integer is a divisor of itself. Integers divisible by 2 are called *even*, and integers not divisible by 2 are called *odd*.

$1, -1, n$, and $-n$ are known as the *trivial divisors* of n. A divisor of n that is not a trivial divisor is known as a *non-trivial divisor* (or *strict divisor*). A non-zero integer with at least one non-trivial divisor is known as a *composite number*, while the *units* -1 and 1 and *prime numbers* have no non-trivial divisors.

A positive divisor of n which is different from n is called a *proper divisor* (or an *aliquot part*) of n.

For example, the number 6 has exactly eight divisors $1, -1$, $2, -2, 3, -3, 6$, and -6, four non-trivial divisors $2, -2, 3$, and -3, and three proper divisors 1, 2, and 3.

In our book, we consider only positive divisors of positive integers.

2.6.2. The *divisor function* (or, more exactly, the *sum of the xth powers of the divisors' function*) $\sigma_x(n)$, for a real or complex number x, is defined as the sum of the xth powers of the positive divisors of n:

$$\sigma_x(n) = \sum_{d|n} d^x.$$

In particular, the function $\sigma_0(n) = \sum_{d|n} 1 = \tau(n)$ is *tau function* (or *the number of divisors' function*): the number of positive integer divisors of a positive integer n; the function $\sigma_1(n) = \sum_{d|n} d = \sigma(n)$ is *sigma function* (or *the sum of divisors' function*): the sum of positive integer divisors of a positive integer n.

For example, $\sigma_0(12) = \tau(12)$ is the number of the divisors of 12:

$$\begin{aligned}\sigma_0(12) &= 1^0 + 2^0 + 3^0 + 4^0 + 6^0 + 12^0\\ &= 1 + 1 + 1 + 1 + 1 + 1 = 6;\end{aligned}$$

$\sigma_1(12) = \sigma(12)$ is the sum of all the divisors:

$$\begin{aligned}\sigma_1(12) &= 1^1 + 2^1 + 3^1 + 4^1 + 6^1 + 12^1\\ &= 1 + 2 + 3 + 4 + 6 + 12 = 28;\end{aligned}$$

$\sigma_2(12)$ is the sum of squares of all the divisors:

$$\begin{aligned}\sigma_2(12) &= 1^2 + 2^2 + 3^2 + 4^2 + 6^2 + 12^2\\ &= 1 + 4 + 9 + 16 + 36 + 144 = 210.\end{aligned}$$

The values of $\sigma_2(n)$ for $n = 1, 2, 3, \ldots$ are 1, 5, 10, 21, 26, 50, 50, 85, 91, 130, 122, 210, 170, 250, 260, ... (sequence A001157 in the OEIS). See also A001157–A001160 for $x = 3, 4, 5$, and A013954–A013972 for $x = 6$ to 24.

The divisor function appears in a number of remarkable identities, including relationships on the Riemann zeta function and the Eisenstein series of modular forms. Divisor functions were studied by Ramanujan, who gave a number of important congruences and identities.

2.6.3. Consider a list of simple properties of the function $\sigma_x(n)$.

Properties of the function $\sigma_x(n)$

1. $\sigma_x(p) = p^x + 1$ for any prime p.
2. $\sigma_x(p^\alpha) = 1 + p^x + p^{2x} + \cdots + p^{\alpha x} = \frac{p^{(\alpha+1)x}-1}{p^x-1}$ for any prime p and any positive integer α.

3. The divisor function $\sigma_x(n)$ is multiplicative: $\sigma_x(mn) = \sigma_x(m)\sigma_x(n)$ if $gcd(m, n) = 1$.
4. $\sigma_x(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = \frac{p_1^{(\alpha_1+1)x}-1}{p_1^x-1} \cdot \frac{p_2^{(\alpha_2+1)x}-1}{p_2^x-1} \cdot \ldots \cdot \frac{p_s^{(\alpha_s+1)x}-1}{p_s^x-1}$.
5. $\sigma_x(n) > n$ for all $n > 1$, $x > 1$.
6. $\sigma_{-x}(n) = \frac{\sigma_x(n)}{n^x}$.

□ The proof of the first property is obvious, as any prime p has exactly two positive integer divisors, 1 and p.

The second property follows from the fact that all positive divisors of p^α are $1, p, p^2, \ldots, p^\alpha$. For the summation, one should just use the formula of the sum of the geometric progression.

For a proof of the third property, we can note that for a multiplicative function $f(n) = n^x$, it holds that $\sigma_x(n) = \sum_{d|n} f(d)$, and so, $\sigma_x(n)$ is multiplicative. Now, the fourth property can be obtained as the combination of the previous two properties.

However, we can just consider two coprimes m and n and note that in this case, one has

$$\sigma_x(nm) = \sum_{d|nm} d^x = \sum_{d_1 d_2|nm} d_1^x d_2^x = \sum_{d_1|n} d_1^x \sum_{d_2|m} d_2^x = \sigma_x(n)\sigma_x(m).$$

Lastly, we can use also the formula $\sum_{d|p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}} f(d) = \prod_{i=1}^s (1 + f(p_i) + f(p_i^2) + \cdots + f(p_i^{\alpha_i}))$ for a multiplicative function $f(n) = n^x$. In fact,

$$\begin{aligned}\sigma_x(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) &= \sum_{d|p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}} d^x \\ &= \prod_{i=1}^s (1 + f(p_i) + f(p_i^2) + \cdots + f(p_i^{\alpha_i})) \\ &= \prod_{i=1}^s (1 + p_i^x + (p_i^x)^2 + \cdots + (p_i^x)^{\alpha_i}) = \prod_{i=1}^s \frac{p_i^{(\alpha_i+1)x} - 1}{p_i^x - 1}.\end{aligned}$$

So, we get the fourth property and, as a corollary, property 3.

For a proof of the last property, one should note that

$$\sigma_{-x}(n) = \sum_{d|n} d^{-x} = \sum_{d|n} \frac{1}{d^x} = \frac{1}{n^x} \sum_{d|n} \frac{n^x}{d^x} = \frac{1}{n^x} \sum_{d|n} \left(\frac{n}{d}\right)^x$$
$$= \frac{1}{n^x} \sum_{d|n} d^x = \frac{\sigma_x(n)}{n^x}.$$

This concludes the proof. □

The sequences A017665–A017712 give the numerators and denominators of $\frac{\sigma_k(n)}{n^k}$ for $k = 1, \ldots, 24$. For example, the numerators of the sums of reciprocals of the divisors of n, i.e., of $\frac{\sigma(n)}{n}$, $n = 1, 2, 3, \ldots$, are 1, 3, 4, 7, 6, 2, 8, 15, 13, 9, 12, 7, 14, 12, 8, ... (sequence A017665 in the OEIS), while the denominators of the sums of reciprocals of the divisors of n, i.e., of $\frac{\sigma(n)}{n}$, $n = 1, 2, 3, \ldots$, are 1, 2, 3, 4, 5, 1, 7, 8, 9, 5, 11, 3, 13, 7, 5, ... (sequence A017666 in the OEIS).

It is a conjecture (Zhi-Wei Sun, 2015) that

- *for each* $k = 2, 3, \ldots$, *all the rational numbers* $\frac{\sigma_k(n)}{n^k} = \sum_{d|n} \frac{1}{d^k}$ $(n = 1, 2, 3, \ldots)$ *have pairwise distinct fractional parts.*

Number of divisor function

2.6.4. The *number of divisors function* (or *tau function*) counts the number of divisors of an integer (including 1 and the number itself). So, the *number of divisors function* $\tau(n) = \sigma_0(n)$ is defined as

$$\tau(n) = \sum_{d|n} 1.$$

The notations $\tau(n)$ (for the German word *Teiler* which means divisors) or $d(n)$ are commonly used to denote the number of divisors function instead of $\sigma_0(n)$.

For example, $\tau(18)$ is the number of divisors of 18:

$$\tau(18) = 1^0 + 2^0 + 3^0 + 6^0 + 18^0$$
$$= 1 + 1 + 1 + 1 + 1 = 5.$$

On the other hand, $\tau(13) = 2$, as the number 13 has exactly two positive integer divisors, 1 and 13.

The values of $\tau(n)$ for $n = 1, 2, 3, \ldots$ are 1, 2, 2, 3, 2, 4, 2, 4, 3, 4, 2, 6, 2, 4, 4, ... (sequence A000005 in the OEIS).

2.6.5. Consider the well-known properties of $\tau(n)$, which are important for our further consideration.

Properties of the function $\tau(n)$

1. $\tau(p) = 2$ for any prime p.
2. $\tau(p^\alpha) = \alpha + 1$ for any prime p and any positive integer α.
3. The function $\tau(n)$ is multiplicative: $\tau(mn) = \tau(m)\tau(n)$ if $gcd(m, n) = 1$.
4. $\tau(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_s + 1)$.
5. $\tau(p_n\#) = 2^n$ for the primorial $p_n\#$.
6. $1 < \tau(n) < n$ for all $n > 2$.
7. $\tau(n)$ is odd if and only if n is a square.
8. $\sum_{d|n} \mu(d)\tau(\frac{n}{d}) = 1$.
9. $\tau(1) + \tau(2) + \cdots + \tau(n) = \lfloor \frac{n}{1} \rfloor + \lfloor \frac{n}{2} \rfloor + \cdots + \lfloor \frac{n}{n} \rfloor$.
10. $\tau(n)$ is the number of ways to write n as a product $n = xy$, $1 \leq x \leq n$, $1 \leq y \leq n$.

□ The first property is obvious, as any prime p has exactly two positive integer divisors, 1 and p. The second property follows from the fact that all positive divisors of p^α are $1, p, p^2, \ldots, p^\alpha$.

For a proof of the third property, we can note that for a multiplicative function $f(n) \equiv 1$, it holds that $\tau(n) = \sum_{d|n} f(d)$, and so, $\tau(n)$ is multiplicative. Now, the fourth property can be obtained as the combination of the previous two properties.

However, if $gcd(m, n) = 1$, it holds that

$$\tau(nm) = \sum_{d|nm} 1 = \sum_{d_1 d_2 | nm} 1 = \sum_{d_1|n} 1 \sum_{d_2|m} 1 = \tau(n)\tau(m).$$

Finally, we can also use the formula $\sum_{d|p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}} f(d) = \prod_{i=1}^{s}(1 + f(p_i) + f(p_i^2) + \cdots + f(p_i^{\alpha_i}))$ for a multiplicative function $f(n) \equiv 1$.

In fact,

$$\begin{aligned}\tau(p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s}) &= \sum_{d|p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s}} 1\\ &= \prod_{i=1}^{s}(1+f(p_i)+f(p_i^2)+\cdots+f(p_i^{\alpha_i}))\\ &= \prod_{i=1}^{s}(1+1+cdots+1) = \prod_{i=1}^{s}(\alpha_i+1).\end{aligned}$$

So, we get the fourth property and, as a corollary, property 3.

This result can be also directly deduced from the fact that all divisors of n are uniquely determined by the distinct tuples

$$(x_1, x_2, \ldots, x_i \ldots, x_s)$$

of integers with $0 \le x_i \le \alpha_i$ (i.e., $\alpha_i + 1$ independent choices for each x_i).

For a non-square integer n, every divisor d of n is paired with divisor $\frac{n}{d}$ of n, and $\tau(n)$ is even; for a square integer, one divisor $\sqrt{n}$ is not paired with a distinct divisor, and $\tau(n)$ is odd. This proves property 7.

Property 8 is just the Dirichlet convolution formula for $F(n) = \tau(n)$ and $f(n) \equiv 1$. □

2.6.6. Consider some equations connected with the number of divisors function.

Solve the equation $\tau(x) = 33,\ 24|x$.

As the number 33 can be represented as a product of several positive integers, not equal to 1, by exactly two ways, i.e., as 33 (one multiplier) or as $3 \cdot 11$ (two multipliers), then the positive integer x has one or two prime divisors. In the first case, we have $x = p^{\alpha}$ and $\tau(x) = \alpha + 1$. So, $\alpha + 1 = 33$, i.e., $\alpha = 32$ and $x = p^{32}$. In the second case, we get $x = p^{\alpha}q^{\beta}$ and $\tau(x) = (\alpha+1)(\beta+1)$. So, $(\alpha+1)(\beta+1) = 3\cdot 11$, i.e., $\alpha = 2$, $\beta = 10$, and $x = p^2q^{10}$. Therefore, all solutions of the equation $\tau(x) = 33$ are the numbers $p^{32},\ p \in P$, and $p^2q^{10},\ p, q \in P,\ p \ne q$.

As $24|x$, then in the prime factorization of x, there are the numbers 2^3 and 3. So, $x = 3^2 \cdot 2^{10}$, i.e., $x = 9216$.

Solve the equation $\tau(2x) = \tau(3x)$.

Represent a positive integer x as $x = 2^\alpha 3^\beta y$, where α and β are non-negative integers and the positive integer y is not divisible by 2 and by 3, i.e., $gcd(2, y) = gcd(3, y) = 1$. In this case, $\tau(2x) = \tau(2^{\alpha+1})\tau(3^\beta)\tau(y)$ and $\tau(3x) = \tau(2^\alpha)\tau(3^{\beta+1})\tau(y)$, and after reduction by $\tau(y)$, we obtain from the equation $\tau(2x) = \tau(3x)$, the equation $\tau(2^{\alpha+1})\tau(3^\beta) = \tau(2^\alpha)\tau(3^{\beta+1})$. Therefore, we get the equality $(\alpha + 2)(\beta + 1) = (\alpha + 1)(\beta + 2)$ or, equivalently, the equality $\alpha = \beta$.

So, all solutions of the equation $\tau(2x) = \tau(3x)$ are positive integers $2^\alpha 3^\alpha y$, where α is a non-negative integer, and the positive integer y is not divisible by 2 and by 3.

2.6.7. The function $\tau(n)$ is a well-known arithmetic function which takes values from 2 for any prime number $p \in P$ till n^ϵ for some special positive integers. So, the asymptotic behavior of $\tau(n)$ is very strange.

In fact, the divisor function satisfies the following inequality:

$$\text{for all } \epsilon > 0, \quad \tau(n) = o(n^\epsilon).$$

More precisely, Severin Wigert showed that

$$\overline{\lim}_{n\to\infty} \frac{\log \tau(n)}{\log n / \log\log n} = \log 2.$$

On the other hand, since there are infinitely many prime numbers,

$$\underline{\lim}_{n\to\infty} \tau(n) = 2.$$

However, Dirichlet showed that on average the order of the divisor function is $x \log x$:

$$\text{For all } x \geq 1, \sum_{n \leq x} \tau(n) = x \log x + (2\gamma - 1)x + O(\sqrt{x}),$$

where γ is the *Euler–Mascheroni constant*: $\gamma = \lim_{n\to\infty}(\sum_{k=1}^{n} \frac{1}{k} - \log n)$. Improving the bound $O(\sqrt{x})$ in this formula is known as *Dirichlet's divisor problem*.

Sum of divisors function

2.6.8. The *sum of divisors function* (or *sigma function*) counts the sum of positive integer divisors of a positive integer n (including 1 and the number itself). So, the *sum of divisors function* $\sigma(n) = \sigma_1(n)$ is defined as

$$\sigma(n) = \sum_{d|n} d.$$

For example, $\sigma(18)$ is the sum of the divisors of 18:

$$\sigma(18) = 1 + 2 + 3 + 6 + 18 = 30.$$

On the other hand, $\sigma(13) = 14$, as the number 13 has exactly two positive integer divisors, 1 and 13.

The values of $\sigma(n)$ for $n = 1, 2, 3, \dots$ are 1, 3, 4, 7, 6, 12, 8, 15, 13, 18, 12, 28, 14, 24, 24, … (sequence A000203 in the OEIS).

2.6.9. Consider a list of the simplest properties of $\sigma(n)$, which are important for our purposes.

Properties of the function $\sigma(n)$

1. $\sigma(p) = p + 1$ for any prime p.
2. $\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1}-1}{p-1}$ for any prime p and any positive integer α.
3. The function $\sigma(n)$ is multiplicative: $\sigma(mn) = \sigma(m)\sigma(n)$ if $gcd(m, n) = 1$.
4. $\sigma(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+1}-1}{p_s-1}$.
5. $\sigma(n) > n$ for all $n > 1$.
6. $\sigma(n)$ is odd if and only if n is a square or twice a square.
7. $\sigma(kn) > k\sigma(n)$ for any $k \geq 2$.
8. $\sum_{d|n} \mu(d)\sigma(\frac{n}{d}) = n$.
9. $\sigma(1) + \sigma(2) + \cdots + \sigma(n) = 1 \cdot \lfloor \frac{n}{1} \rfloor + 2 \cdot \lfloor \frac{n}{2} \rfloor + \cdots + n \cdot \lfloor \frac{n}{n} \rfloor$.
10. $\sigma(n)$ is the total number of parts in the partitions of n into equal parts.

□ In fact, for prime p, the result is obvious, as any prime p has exactly two divisors 1 and p. For any prime p and any natural α, the divisors of p^α are $1, p, p^2, \ldots, p^\alpha$. In this case

$$\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}.$$

For a proof of the third property, we can note that for a multiplicative function $f(n) = n$, it holds that $\sigma(n) = \sum_{d|n} f(d)$, and so, $\sigma(n)$ is multiplicative. Now, the fourth property can be obtained as the combination of the previous two properties.

However, we can just consider two coprimes m and n and note that in this case, one has

$$\sigma(nm) = \sum_{d|nm} d = \sum_{d_1 d_2 | nm} d_1 d_2 = \sum_{d_1|n} d_1 \sum_{d_2|m} d_2 = \sigma(n)\sigma(m).$$

Finally, we can use also the formula $\sum_{d|p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s}} f(d) = \prod_{i=1}^s (1 + f(p_i) + f(p_i^2) + \cdots + f(p_i^{\alpha_i}))$ for a multiplicative function $f(n) = n$. In fact,

$$\begin{aligned}\sigma(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) &= \sum_{d|p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s}} d = \sum_{d|p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s}} 1 \\ &= \prod_{i=1}^{s}(1 + f(p_i) + f(p_i^2) + \cdots + f(p_i^{\alpha_i})) \\ &= \prod_{i=1}^{s}(1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}) = \prod_{i=1}^{s} \frac{p_i^{(\alpha_i+1)x} - 1}{p_i^x - 1}.\end{aligned}$$

So, we get the fourth property and, as a corollary, property 3.

For a proof of property 6, it is sufficient to note that for any odd prime p and any even α, the sum $1 + p + p^2 + \cdots + p^\alpha$ is odd; as for the only even prime 2, the sum $1 + 2 + 2^2 + \cdots + 2^\alpha$ is odd for any positive integer α.

Property 8 is just the Dirichlet convolution formula for $F(n) = \sigma(n)$ and $f(n) = n$. □

2.6.10. Consider some equations connected with the sigma function.

For example, solve the equation $\sigma(x) = x + 3$.

It is easy to see that $x \neq 1$. Then, we have at least two positive integers divisors of x: 1 and x. As the sum of divisors of x is $x+3$, the number x has exactly one additional positive integer divisor 2. It is possible only in the case $x = 4$.

So, the only solution of the equation $\sigma(x) = x + 3$ is the number 4.

2.6.11. The behavior of the sigma function is irregular. The asymptotic growth rate of the sigma function can be expressed (Grönwall, 1913) by

$$\overline{\lim}_{n\to\infty} \frac{\sigma(n)}{n \log\log n} = e^{\gamma},$$

where γ is the Euler–Mascheroni constant.

In 1915, Ramanujan proved that under the assumption of the Riemann hypothesis, the inequality

$$\sigma(n) < e^{\gamma} n \log\log n,$$

(*Robin's inequality*) holds for all sufficiently large n. The largest known value that violates the inequality is $n = 5040$.

In 1984, Robin proved that the inequality is true for all $n > 5040$ if and only if the Riemann hypothesis is true. This is *Robin's theorem* and the inequality became known after him.

Robin also proved, unconditionally, that the inequality

$$\sigma(n) < e^{\gamma} n \log\log n + \frac{0.6483\ n}{\log\log n}$$

holds for all $n \geq 3$. (See [Rama00] and [Robi84].)

On average, the order of the sigma function is $\frac{\pi^2}{12}x^2$:

$$\sum_{n=1}^{x} \sigma(n) = \frac{\pi^2}{12} x^2 + O(x \log x) \quad \text{for all } x \geq 1.$$

We prove this result later.

Aliquot sum function

2.6.12. The *aliquot sum function* (or *aliquot sum*, *restricted divisor function*) $s(n)$ of n is the sum of the proper divisors (that is, the divisors excluding n itself):

$$s(n) = \sum_{d|n,\ d\neq n} d.$$

In other words, $s(n) = \sigma(n) - n$.

This function is the one used to recognize perfect numbers which are the positive integers n for which $s(n) = n$. If $s(n) > n$, then n is an *abundant number*, and if $s(n) < n$, then n is a *deficient number*.

For example, the aliquot sum $s(12)$ of proper divisors of the number 12 is

$$s(12) = 1 + 2 + 3 + 4 + 6 = 16.$$

On the other hand, $s(18) = 1 + 2 + 3 + 6 = 12$.

The values of $s(n)$ for $n = 1, 2, 3, \ldots$ are 0, 1, 1, 3, 1, 6, 1, 7, 4, 8, 1, 16, 1, 10, 9, ... (sequence A001065 in the OEIS).

2.6.13. It is easy to obtain some values of $s(n)$:

- *For any prime p and any positive integer α, it holds that* $s(p) = 1$ and $s(p^\alpha) = \frac{p^\alpha - 1}{p-1}$.

In particular,

- *if $n = 2^k$, then $s(n) = n - 1$.*

This property makes n *almost perfect.*

It is obvious that

- *the function $s(n)$ gives the total number of parts in all partitions of n into equal parts that do not contain 1 as a part.*

□ In fact, if d is a proper divisor of n, then $n = dk$ and, therefore, n can be represented as a sum of d equal parts: $n = k + k + \cdots + k$. As $d \neq n$, then $k \neq 1$. □

As $s(1) = 0$, we can state that

- *the function $s(n)$ is not multiplicative.*

The function $s(n)$ is also used to define the aliquot sequence of a number.

An *aliquot sequence* of a given positive integer n is a sequence of non-negative integers in which each term is the sum of the proper divisors of the previous term.

In terms of the aliquot sum function $s(n)$, the aliquot sequence of a number n is defined in the following way:

$$s^0(n) = n,\ s^1(k) = s(n), \dots, s^k(n) = s(s^{k-1}(n)), \dots .$$

For example, the aliquot sequence of 10 is 10, 8, 7, 1, 0 because $s(10) = 5 + 2 + 1 = 8$, $s(8) = 4 + 2 + 1 = 7$ and $s(7) = 1$, $s(1) = 0$. We consider these and other questions in Chapter 5.

Unitary divisor function

2.6.14. A *unitary divisor* of a positive integer n is defined as a positive integer divisor d of n for which $gcd(d, \frac{n}{d}) = 1$.

For example, the divisors of 12 are $1, 2, 3, 4, 6, 12$, so the unitary divisors are $1, 3, 4, 12$.

The *unitary divisor function* (or *the sum of the xth powers of the unitary divisors function*) $\sigma_x^*(n)$ is the analog of the divisor function $\sigma_x(n)$ for unitary divisors. It counts the sum of the xth powers of unitary divisors d^* of a positive integer n:

$$\sigma_x^*(n) = \sum_{d^*|n} (d^*)^x.$$

As in the case of the usual divisor function, $\sigma_0^*(n)$ is commonly written as $\tau^*(n)$, while $\sigma_1^*(n)$ is commonly written as $\sigma^*(n)$.

For example, having four unitary divisors $1, 3, 4$, and 12 of 12, we get $\sigma_0^*(12) = 4$, while $\sigma_1^*(12) = \sigma^*(12) = 1 + 3 + 4 + 12 = 20$.

The numbers $\tau^*(n)$ of unitary divisors of $n = 1, 2, 3, \dots$ are 1, 2, 2, 2, 2, 4, 2, 2, 2, 4, 2, 4, 2, 4, 4, ... (sequence A034444 in the OEIS).

The sums $\sigma^*(n)$ of unitary divisors of $n = 1, 2, 3, \dots$ are 1, 3, 4, 5, 6, 12, 8, 9, 10, 18, 12, 20, 14, 24, 24, ... (sequence A034444 in the OEIS).

The sums $\sigma_2^*(n)$ of squares of unitary divisors of $n = 1, 2, 3, \dots$ are 1, 5, 10, 17, 26, 50, 50, 65, 82, 130, 122, 170, 170, 250, 260, ... (sequence A034676 in the OEIS).

2.6.15. Given the prime factorization $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ of n, the divisor $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}$ of n is a unitary divisor of n if each β_i is 0 or α_i.

For a prime p, the unitary divisors are 1 and p, so

$$\sigma_x^*(p) = 1 + p^x,$$

in particular, $\tau^*(p) = \tau(p) = 2$, and $\sigma^*(p) = \sigma(p) = p + 1$.

For a prime power p^α, the unitary divisors are 1 and p^α (Cohen, 1990), so

$$\sigma_x^*(p^\alpha) = p^{x\alpha} + 1,$$

in particular, $\tau^*(p^\alpha) = 2$, while $\sigma^*(p^\alpha) = p^\alpha + 1$.

It is easy to check that

- *the function $\sigma_x^*(n)$ is multiplicative.*

□ In fact, for any coprime m and n, it holds that

$$\sigma_x^*(nm) = \sum_{d^*|nm} (d^*)^x = \sum_{d_1^* d_2^*|nm} (d_1^*)^x (d_2^*)^x$$
$$= \sum_{d_1^*|n} (d_1^*)^x \sum_{d_2^*|m} (d_1^*)^x = \sigma_x^*(n)\sigma_x^*(m). \qquad \square$$

So, now we can state that

- *$\sigma_x^*(n)$ can be computed using the formula*

$$\sigma_x^*(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) = (1 + p_1^{x\alpha_1})(1 + p_2^{x\alpha_2}) \cdots (1 + p_2^{x\alpha_s}).$$

In particular,

$$\tau^*(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) = 2^s,$$

i.e., *the number of unitary divisors of n is given by 2^s, where s is the number of different primes dividing n.*

Moreover,

$$\sigma^*(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) = (1 + p_1^{\alpha_1})(1 + p_2^{\alpha_2}) \cdots (1 + p_2^{\alpha_s}).$$

If n is square-free, then any divisor of n is a unitary divisor, and so, $\sigma_x(n) = \sigma_x^*(n)$.

One can state that $\tau^*(n)$ gives also the number of square-free divisors of n.

2.6.16. A positive integer divisor d of a positive integer n is called a *bi-unitary divisor* if the greatest common unitary divisor of d and $\frac{n}{d}$ is 1. The function $\sigma_x^{**}(n)$ is defined as the sum of xth powers of bi-unitary divisors d^{**} of n:

$$\sigma_x^{**}(n) = \sum_{d^{**}|n} (d^{**})^x.$$

For a prime power p^α, the bi-unitary divisors are the powers $1, p, p^2, \ldots, p^\alpha$, except for $p^{\frac{\alpha}{2}}$ when α is even (Cohen, 1990, [Cohe90]).

The sum $\sigma_x^{**}(n)$ of x-powers of bi-unitary divisors d^{**} of n is a multiplicative function with $\sigma_x^{**}(p^\alpha) = \frac{p^{x\alpha+1}-1}{p-1}$ if α is odd and $\sigma_x^{**}(p^\alpha) = \frac{p^{x\alpha+1}-1}{p-1} - p^{\frac{x\alpha}{2}}$ if α is even. In particular,

$$\tau^{**}(p^\alpha) = \alpha + 1 \quad \text{for } \alpha = 2k+1,$$

$$\text{and} \quad \tau^{**}(p^\alpha) = \alpha \quad \text{for } \alpha = 2k;$$

$$\sigma^{**}(p^\alpha) = \frac{p^{x\alpha+1} - 1}{p - 1} \quad \text{for } \alpha = 2k+1,$$

$$\text{and} \quad \sigma^{**}(p^\alpha) = \frac{p^{x\alpha+1} - 1}{p - 1} - p^{\frac{x\alpha}{2}}, \quad \text{for } \alpha = 2k.$$

The numbers of the bi-unitary divisors of $n = 1, 2, 3, \ldots$ are 1, 2, 2, 2, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, 4, …. (sequence A286324 in the OEIS).

The sums of the bi-unitary divisors of $n = 1, 2, 3, \ldots$ are 1, 3, 4, 5, 6, 12, 8, 15, 10, 18, 12, 20, 14, 24, 24, … (sequence A188999 in the OEIS).

Mean values of divisor functions

2.6.17. In number theory, there are many famous arithmetic functions which play important role in arithmetic, number theory, and discrete mathematics in general. But, as a rule, the behavior of an arithmetic function f is very irregular, and researching the asymptotic behavior of most arithmetic functions is difficult.

But we can obtain useful information about the asymptotic behavior of f "on average," which means by research of the function

$$F(x) = \sum_{1 \le n \le x} f(n),$$

which is called the *mean value* of the function f on the interval $[1, x]$. As a rule, this function behaves more smoothly.

Recall that $f(x) = O(g(x))$ if for some x_0, we have for any $x \ge x_0$, the function $g(x) > 0$ and $|f(x)| \le Cg(x)$ for some positive constant C.

2.6.18. For the sum of divisors function $\sigma(n)$, we can obtain the following result.

Theorem (mean value of $\boldsymbol{\sigma(n)}$). *For a given positive integer N, one has*

$$\sum_{n=1}^{N} \sigma(n) = \frac{\pi^2}{12} N^2 + O(N \log N).$$

□ We have

$$\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} \sum_{d|n} d = \sum_{n=1}^{N} \sum_{d|n} \frac{n}{d} = \sum_{d=1}^{N} \sum_{n \le N, d|n} \frac{n}{d}.$$

As

$$\sum_{n \le N, d|n} \frac{n}{d} = \sum_{s=1}^{\left\lfloor \frac{N}{d} \right\rfloor} s = \frac{1}{2} \left\lfloor \frac{N}{d} \right\rfloor \left(\left\lfloor \frac{N}{d} \right\rfloor + 1 \right),$$

we obtain that

$$\begin{aligned}\sum_{n=1}^{N} \sigma(n) &= \frac{1}{2} \sum_{d=1}^{N} \left(\frac{N}{d} - \left\{ \frac{N}{d} \right\} \right) \left(\frac{N}{d} + 1 - \left\{ \frac{N}{d} \right\} \right) \\ &= \frac{N^2}{2} \sum_{d=1}^{\infty} \frac{1}{d^2} - \frac{N^2}{2} \sum_{d=N+1}^{\infty} \frac{1}{d^2} + O\left(N \sum_{d=1}^{N} \frac{1}{d} \right).\end{aligned}$$

As

$$\sum_{1}^{\infty} \frac{1}{d^2} = \zeta(2) = \frac{\pi^2}{6}, \quad \text{and}$$

$$\sum_{N+1}^{\infty} \frac{1}{d^2} < \sum_{n+1}^{\infty} \left(\frac{1}{d-1} - \frac{1}{d} \right) = \frac{1}{N} = O\left(\frac{1}{N} \right),$$

we obtain that

$$\sum_{n=1}^{N} \sigma(n) = \frac{N^2 \pi}{12} + O\left(N \log N\right).$$

This concludes the proof. □

So, we have obtained that "on average" the sum of divisors function $\sigma(n)$ behaves as Cn, where the constant $C = \frac{\pi^2}{12} \approx 0.82246\ldots$.

2.6.19. In order to obtain the mean value of the function $\tau(n)$, we need an additional result about the mean value of the arithmetic function $f(n) = \frac{1}{n}$:

- *For any positive integer N, it holds that*

$$\sum_{k=1}^{N} \frac{1}{k} = \log N + O(1).$$

□ It is easy to see that

$$\frac{1}{k} \leq \int_{k}^{k+1} \frac{dx}{x} \leq \frac{1}{k+1}, \text{ i.e. } 0 \leq \frac{1}{k} - \int_{k}^{k+1} \frac{dx}{x} \leq \frac{1}{k} - \frac{1}{k+1},$$

and

$$0 \leq \sum_{k=1}^{N} \frac{1}{k} - \int_{1}^{N} \frac{dx}{x} \leq 1 \frac{1}{N+1} + \int_{N}^{N+1} \frac{dx}{x}$$

$$= 1 + O\left(\frac{1}{N+1} \right) = O(1).$$

Now, we can write that

$$\sum_{k=1}^{N} \frac{1}{k} = \log N + O(1).$$

□

Theorem (mean value of $\tau(n)$). *For any positive integer N, it holds that*

$$\sum_{n=1}^{N} \tau(n) = N \log N + O(N).$$

□ We have

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \sum_{d|N} 1 = \sum_{nm \le N} 1 = \sum_{1 \le k \le N} \left\lfloor \frac{N}{k} \right\rfloor$$
$$= N \sum_{k=1}^{N} \frac{1}{k} + O(N) = N \log N + O(N).$$

This conclude the proof. □

2.6.20. In a similar way, we can obtain better results on the mean values of $\frac{1}{n}$ and $\tau(n)$, but the proofs become more complicated. In fact,

- *for any positive integer N, it holds that*

$$\sum_{k=1}^{N} \frac{1}{k} = \log N + \gamma + O\left(\frac{1}{N}\right),$$

where $\gamma = \lim_{N\to\infty}(\sum_{n=1}^{N} \frac{1}{n} - \int_1^N \frac{dx}{x}) = 0.57721\ldots$ is the Euler–Mascheroni constant.

□ It is easy to see that

$$\frac{1}{k} \le \int_k^{k+1} \frac{dx}{x} \le \frac{1}{k+1},$$

i.e.,

$$0 \le \frac{1}{k} - \int_k^{k+1} \frac{dx}{x} \le \frac{1}{k} - \frac{1}{k+1}, \quad \text{and}$$
$$0 \le \sum_{k=1}^{N} \frac{1}{k} - \int_1^N \frac{dx}{x} \le 1 + O\left(\frac{1}{N}\right).$$

So, as $N \to \infty$, the value $\sum_{k=1}^{N} \frac{1}{k} - \int_1^N \frac{dx}{x} = \sum_{k=1}^{N} \frac{1}{k} - \log N$ is convergent to some constant γ. Now, we can write that

$$\sum_{k=1}^{N} \frac{1}{k} = \log N + \gamma + O\left(\sum_{k=N+1}^{\infty} \frac{1}{k} - \int_{N+1}^{\infty} \frac{dx}{x} \right),$$

where the last error term is, in view of the previous consideration, $O(\frac{1}{N+1})$, i.e., $O(\frac{1}{N})$. □

Theorem (mean value of $\boldsymbol{\tau(n)}$-I). *For any positive integer* N, *it holds that*

$$\sum_{n=1}^{N} \tau(n) = N \log N + (2\gamma - 1) + O(\sqrt{N}).$$

□ We have

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \sum_{d|N} 1 = \sum_{nm \le N} 1 = 2 \sum_{1 \le k \le \sqrt{N}} \left\lfloor \frac{N}{k} \right\rfloor - \left\lfloor \sqrt{N} \right\rfloor^2$$

$$= 2N \sum_{k=1}^{\sqrt{N}} \frac{1}{k} + O(\sqrt{N}) - N = 2N(\log \sqrt{n}) + \gamma$$

$$+ O\left(\frac{1}{\sqrt{N}} \right)) - N + O(\sqrt{N})$$

$$= N \log N + (2\gamma - 1) + O(\sqrt{N}).$$

This concludes the proof. □

So, we have obtained that "on average," the number of divisors function $\tau(n)$ behaves as $\log n$.

This classical result was obtained by P. Dirichlet in the middle of the 19th century (1849), and the problem to determine the precise order of magnitude of the error term $\Delta(x) = \sum_{n \le x} \tau(n)$ as $x \to +\infty$ is known as *Dirichlet divisor problem.*

2.6.21. Note that the mean value of $\tau(n)$ is the number of positive integer points under the hyperbola $x_1 x_2 = x$. Hence, the Dirichlet divisor problem is an example of a problem about calculating the amount of integer points in some region. One of the most famous examples in this area is the *Gauss circle problem* concerning the calculation of the amount of integer points in a circle.

The classical result by Gauss gives the asymptotic formula for the amount of integer points in the circle of radius $\sqrt{x}$:

$$\sum_{x_1^2+x_2^2\le x} 1 = \pi x + O(\sqrt{x}).$$

2.6.22. Consider now one more arithmetic function,

$$\tau_k(n) = \sum_{n_1 \dots n_k = n} 1,$$

which is the number of representations of positive integer number n as a product of k positive integer factors.

We can see that for $k = 2$, the function $\tau_2(n)$ coincides with the function $\tau(n)$, and hence, the function $\tau_k(n)$ is a generalization of the divisor function.

Consider the function

$$D_k(x) = \sum_{n\le x} \tau_k(n) = \sum_{n_1 \dots n_k \le x} 1$$

— the mean value of the function $\tau_k(n)$. It is the amount of positive integer points under the hyperbolic surface $x_1 \dots x_k = x$.

Elementary arguments allow us to obtain this asymptotic formula for $D_k(x)$:

$$D_k(x) = \sum_{n\le x} \tau_k(n) = xP_k(\log x) + \Delta_k(x),$$

where P_k is a polynomial of degree $k-1$, and $\Delta_k(x)$ is an error term.

The estimation of the error term is known as the *multidimensional Dirichlet divisor problem.* An extension of Dirichlet's method gives such a value of $\Delta_k(x)$:

$$\Delta_k(x) = O(x^{1-1/k} \log^{k-2} x).$$

For detailed proofs, references, and additional information, see, for example, [Apos86], [Buch09], [Cohe60], [Cohe90], [Deza18], [Deza21], [DeKo13], [DeKo18], [Dick27], [Guy94], [HaWr79], [MSC96], [Ivic85], [Rama00], [Robi84], [Sloa22], and [Wiki22].

Exercises

1. Calculate:

   (a) $\tau(100)$;
   (b) $\sigma(50)$;
   (c) $\tau(\sigma(12)!)$;
   (d) $\tau(\sigma(3!))$;
   (e) $\tau(\frac{10!}{5!5!})$;
   (f) $\tau(\frac{12!}{4!8!})$;
   (g) $\sigma(\frac{6!}{3!3!})$;
   (h) $\sigma(\frac{10!}{5!5!})$;
   (i) $\sigma(\tau(5!))$;
   (j) $\sigma(\tau(3!))$;
   (k) $\sigma(\tau(10)!)$;
   (l) $\sigma(\tau(16)!)$.

2. Check if the divisibility exists:

   (a) $\tau(\sigma(37))!$ by $(\sigma(11))^7$;
   (b) $\tau(\sigma(41))!$ by $(\sigma(7))^6$;
   (c) $\sigma(\tau(12)!)$ by $(\tau(7))^{10}$;
   (d) $\sigma(\tau(24)!)$ by $(\tau(4))^{12}$.

3. Solve the equation:

   (a) $\tau(x) = 2$;
   (b) $\tau(x) = 11$;
   (c) $\tau(x) = 13$;
   (d) $\tau(x) = 17$;
   (e) $\tau(x) = 101$;
   (f) $\tau(x) = p$;
   (g) $\tau(x) = 6$;
   (h) $\tau(x) = 10$;
   (i) $\tau(x) = pq$;
   (j) $\tau(x) = 20$;
   (k) $\tau(x) = 50$;
   (l) $\tau(x) = pq^2$;
   (m) $\tau(3x) = \tau(13x)$;
   (n) $\tau(5x) = \tau(17x)$;
   (o) $\tau(11x) = \tau(13x)$;
   (p) $\tau(3x) = \tau(7x)$;
   (q) $\tau(3x) = \tau(5x)$;
   (r) $\tau(px) = \tau(qx)$;
   (s) $\sigma(x) = 3$;
   (t) $\sigma(x) = 4$;
   (u) $\sigma(x) = 6$;
   (v) $\sigma(x) = x + 6$;
   (w) $\sigma(x) = x + 5$;
   (x) $\sigma(x) = x + 7$.

4. Find a positive integer n such that $n = p^\alpha q^\beta$, $\tau(n) = 6$, and $\sigma(n) = 28$. Find a positive integer n such that $n = 32pq$ and $\sigma(n) = 3n$. Find a positive integer n such that $n = 32pq$ and $\sigma(n) = \frac{27n}{10}$. Find $\tau(n^3)$ if $\tau(n^2) = 15$.
5. Find the smallest positive integer having 10 positive integer divisors and all two-digit positive integers having 10 positive integer divisors.

6. Prove:
   (a) $\tau(1)+\tau(2)+\cdots+\tau(n)=\lfloor\frac{n}{1}\rfloor+\lfloor\frac{n}{2}\rfloor+\cdots+\lfloor\frac{n}{n}\rfloor$;
   (b) $\sigma(1)+\sigma(2)+\cdots+\sigma(n)=1\cdot\lfloor\frac{n}{1}\rfloor+2\cdot\lfloor\frac{n}{2}\rfloor+\cdots+n\cdot\lfloor\frac{n}{n}\rfloor$.
7. Prove:
   (a) $2|\tau(n)\Rightarrow n\neq a^2$;
   (b) $(\tau(m^n),n)=1$;
   (c) $n>2\Rightarrow\tau(n)<n$;
   (d) $n\in S\Rightarrow\sigma(n)>n+\sqrt{n}$;
   (e) $(a,b)>1\Rightarrow\tau(a)\tau(b)>\tau(ab)$;
   (f) $(a,b)>1\Rightarrow\sigma(a)\sigma(b)>\sigma(ab)$;
   (g) $\prod_{d|n}d=n^{0.5\tau(n)}$.
8. Find all n such that n is product of all its proper divisors. Prove that $n\in\{p^3,pq\}$.
9. Prove that $\tau(mn)\leq\tau(m)\tau(n)$.
10. Let $\sigma_k(n)=\sum_{d|n}d^k$, $k\in\mathbb{N}$. Find $\sigma_2(6)$, $\sigma_3(5)$. Prove that $\sigma_k(p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s})=\frac{p_1^{(\alpha_1+1)k}-1}{p_1^k-1}\cdot\ldots\cdot\frac{p_s^{(\alpha_s+1)k}-1}{p_s^k-1}$. Prove that $\sigma_k(mn)\leq\sigma_k(m)\sigma_k(n)$.
11. Let $\tau_k(n)=\sum_{n=n_1\cdot\ldots\cdot n_k}1$. Find $\tau_2(3)$, $\tau_3(6)$, and $\tau_4(5)$. Prove that $\tau_2(n)=\tau(n)$. Check for $n=1,2,3,\ldots,20$ that $\tau_k(p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s})=\frac{(\alpha_1+k-1)!}{(k-1)!\alpha_1!}\cdot\ldots\cdot\frac{(\alpha_s+k-1)!}{(k-1)!\alpha_s!}$.

References

[Apos86], [BaCo87], [BrSc95], [Buch09], [Chan70], [Cohe60], [Cohe90], [CoGu96], [Dave99], [Deza17], [Deza18], [Deza21], [Dick05], [Eule48], [FlLu00], [Ford99], [Gaus01], [Guy94], [HaWr79], [Ingh32], [IrRo90], [Ivic85], [Kara83], [KGP94], [Lagr70], [Malc86], [MaSt15], [MSC96], [Moze09], [Nage51], [Ore48], [Plou92], [Rama00], [Sier64], [Sloa22], [Weis22], [Wiki22].

Chapter 3

Perfect Numbers

3.1. History of the Question

3.1.1. Many ancient cultures were concerned with the relationship of a number with the sum of its divisors often giving mystic interpretations. Here, we are concerned with one such relationship.

A *perfect number* is a positive integer that is equal to the sum of its positive divisors, excluding the number itself, i.e., as the sum of its proper divisors.

For instance, 6 has divisors 1, 2, and 3 (excluding itself), and $1 + 2 + 3 = 6$, so 6 is a perfect number.

The number 12 has proper divisors 1, 2, 3, 4, and 6, and $1 + 2 + 3 + 4 + 6 > 12$; it means that 12 is an *abundant number*.

The number 4 has proper divisors 1 and 2, and $1 + 2 < 4$, so 4 is a *deficient number*.

It is easy to check that 6 is the first perfect number.

The second perfect number is 28: $28 = 1 + 2 + 4 + 7 + 14$.

The next two are 496 and 8128: $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$; and $8128 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064$.

3.1.2. There is not much information regarding the discovery of perfect numbers. It is said that perhaps the Egyptians may have discovered them. Despite knowing the existence of perfect numbers, it was only the Greeks who were eager to study more about these numbers. Perfect numbers were studied by Pythagoras and his followers.

However, the Pythagoreans were most interested in the occult, mystical, and numerological properties of the perfect and other classes of numbers, and they did little of mathematical significance with them.

It was around 300 BC when Euclid wrote his *Elements* that the first real result was obtained. Although Euclid concentrated on geometry, many number theoretical results can be found in his text.

In fact, in Euclid's *Elements* (VII.22), the first formal definition of perfect numbers appeared; in this book, a perfect number is called *perfect, ideal*, or *complete number.*

Moreover, Euclid proved that $2^{p-1}(2^p-1)$ *is an even perfect number whenever* 2^p-1 *is prime* (*Elements*, Proposition IX.36).

Later, Nicomachus from Gerasa (circa AD 60–120) and Alhazen (circa AD 1000) conjectured that *every even perfect number is of the form* $2^{p-1}(2^p-1)$*, where* 2^p-1 *is prime*, but they were not able to prove this result.

It was not until the 18th century, over two millennia after Euclid, that L. Euler (1707–1783) proved that the formula $2^{p-1}(2^p-1)$, $2^p-1 \in P$ will yield all the even perfect numbers, i.e., that *all even perfect numbers are of this form.* This is known now as the *Euclid–Euler theorem.*

The first four perfect numbers are generated by the formula $2^{p-1}(2^p-1)$, with p a prime number, as follows:

for $p=2$: $2^1(2^2-1)=2\cdot 3=6$;
for $p=3$: $2^2(2^3-1)=4\cdot 7=28$;
for $p=5$: $2^4(2^5-1)=16\cdot 31=496$;
for $p=7$: $2^6(2^7-1)=64\cdot 127=8128$.

There four numbers were the only ones known to early Greek mathematics.

They were given in the *Arithmetic* of Nicomachus of Gerasa.

Nicomachus noted 8128 as early as around AD 100. He stated also (without proof) that every perfect number is of the form $2^{n-1}(2^n-1)$, where $2^n - 1$ is a prime.

He also says (wrongly) that the perfect numbers end in 6 or 8 alternately. (The first five perfect numbers end with digits 6, 8, 6, 8, and 6, but the sixth also ends in 6.)

Philo of Alexandria (circa 20 BC – AD 50) in his first-century book *On the creation* mentioned perfect numbers, claiming that the world was created in 6 days and the moon orbits in 28 days because 6 and 28 are perfect.

Origen (circa AD 184–253) added the observation that there are only four perfect numbers that are less than 10000.

St. Augustine (354–430) considered perfect numbers in *City of God* (Book XI, Chapter 30) in the early fifth century AD, repeating the claim that God created the world in 6 days because 6 is the smallest perfect number.

In the 13th century, the Egyptian mathematician Ismail ibn Fallus (1194–1252) mentioned the next three perfect numbers (33550336, 8589869056, and 137438691328) and listed a few more which are now known to be incorrect.

The first known European mention of the fifth perfect number is a manuscript written between 1456 and 1461 by an unknown mathematician. The fifth perfect number 33550336 corresponding to $p = 13$ was studied by Regiomontanus (1436–1476), a mathematician, astrologer, and astronomer of the German Renaissance.

In the 16th century, the German scientist Scheibel described two more, sixth and seventh, perfect numbers, 8589869056 and 137438691328. They correspond to $p = 17$ and $p = 19$.

Many writers felt that the numbers of the form $2^n - 1$ were prime for all primes n, but in 1536, Hudalricus Regius showed that $2^{11} - 1 = 2047$ was not prime; it is $23 \cdot 89$.

By 1603, the Italian mathematician P. Cataldi (1548–1626) had correctly verified that $2^{17} - 1$ and $2^{19} - 1$ were both primes (and so identified the sixth (8589869056) and the seventh (137438691328) perfect numbers) and also proved that every perfect number obtained from Euclid's rule ends with a 6 or an 8.

Moreover, he (incorrectly) stated that $2^n - 1$ was also prime for $23, 29, 31$, and 37.

In 1640, Pierre Fermat (1607–1665) showed that P. Cataldi was wrong about 23 and 37; then, L. Euler in 1732 showed that P. Cataldi was also wrong about 29. Sometime later, L. Euler (1750) showed that Cataldi's assertion about 31 was correct. So, the eighth prime $2147483647 = 2^{31} - 1$ of the form $2^p - 1$ was found as well as the eighth perfect number $230584\ldots 952128 = 2^{30}(2^{31} - 1)$ (19 digits).

Although Nicomachus and Origen had stated that all perfect numbers were of the form $2^{n-1}(2^n - 1)$, where $2^n - 1$ is prime, it was not until the 18th century that L. Euler proved that the formula $2^{p-1}(2^p - 1)$ will yield all the even perfect numbers.

So, around Euler's time, exactly eight perfect numbers were known. They corresponded to the first eight primes, $2^p - 1$ with $p = 2, 3, 5, 7, 13, 17, 19, 31$.

3.1.3. Though the numbers of the form $2^n - 1$ were studied by many mathematicians, they were eventually named after Marin Mersenne (1588–1648), a French monk and mathematician, whose works touched a wide variety of fields.

M. Mersenne was born in Sarthe, France. He was educated at the Jesuit College of La Flèche.

Between 1614 and 1618, he taught Theology and Philosophy at Nevers, but he returned to Paris and settled at the convent of L'Annonciade in 1620. There, he studied mathematics and met with René Descartes, Étienne Pascal, Pierre Petit, Gilles de Roberval, Thomas Hobbes, and Nicolas-Claude Fabri de Peiresc. He corresponded with Giovanni Doni, Jacques Alexandre Le Tenneur, Constantijn Huygens, Galileo Galilei, and other scholars in Italy, England, and the Dutch Republic.

In 1635, he set up the informal Académie Parisienne (Academia Parisiensis), which had nearly 140 correspondents, including astronomers and philosophers, as well as mathematicians.

He was not afraid to cause disputes among his learned friends in order to compare their views, notable among which were disputes between R. Descartes, P. de Fermat, and J. de Beaugrand. In 1635, Mersenne met with Tommaso Campanella. During 1643–1644, Mersenne also corresponded with the German Socinian Marcin Ruar, concerning the Copernican ideas of Pierre Gassendi.

M. Mersenne discussed numbers of the form $2^n - 1$ in his work *Cogita physico mathematics* (1644) and stated conjectures about the number's occurrence.

One of his most famous conjectures is called the *Mersenne conjecture*:

- $2^n - 1$ *is prime for* $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ *and is composite for all other integers* $2 \le n \le 257$.

It is obvious, that M. Mersenne could not have tested all of these numbers. It took three centuries and several mathematical discoveries (such as the *Lucas–Lehmer test*), before the exponents in Mersenne's conjecture had been completely checked.

It was determined that M. Mersenne had made five errors (three primes, for $n = 61, 89, 107$, omitted and two composites, for $n = 67, 257$, listed), and the correct list is

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, \text{ and } 127.$$

Primality of the number $2147483647 = 2^{31} - 1$ was proved by L. Euler (1750).

Primality of a 19-digit number $2305843009213693951 = 2^{61} - 1$ was proved by the Russian mathematician I. Pervushin (1883). So, in 1883, a new (in fact, the ninth) perfect number $265845 \ldots 842176 = 2^{60}(2^{61} - 1)$ (34 digits) was found.

R. E. Powers showed that a 27-digit number $2^{89} - 1$ is prime (1911), as well as a 33-digit number $2^{107} - 1$ (1913). These Mersenne primes form the ninth and the tenth perfect numbers $191561 \ldots 169216 = 2^{88}(2^{89} - 1)$ (54 digits) and $131640 \ldots 728128 = 2^{106}(2^{107} - 1)$ (65 digits).

É. Lukas (1876) showed that $2^{127} - 1 \in P$. This 39-digit Mersenne number is the largest prime number found in the pre-computer era. The corresponding perfect number (in fact, the 11th) $144740\ldots 152128 = 2^{126}(2^{127} - 1)$ has 77 digits.

The next result was obtained only in 1952 by R. M. Robinson, who with the help of computers managed to prove primality of Mersenne numbers $2^{521} - 1$ (157 decimal digits), $2^{607} - 1$ (183 decimal digits), $2^{1279} - 1$ (386 decimal digits), $2^{2203} - 1$ (664 decimal digits), and $2^{2281} - 1$ (687 decimal digits). So, four new perfect numbers (in fact, the 13th–16th) $235627\ldots 646976 = 2^{520}(2^{521} - 1)$ (314 digits), $141053\ldots 328128 = 2^{606}(2^{607} - 1)$ (366 digits), $541625\ldots 291328 = 2^{1278}(2^{1279} - 1)$ (770 digits), and $108925\ldots 782528 = 2^{2202}(2^{2203} - 1)$ (1327 digits) were found.

So, the Mersenne's conjecture was not completely correct, but his name is still attached to the numbers of the form $2^n - 1$.

3.1.4. Where did M. Mersenne get his list? Perhaps, we find a hint in this quote. In a letter to Tanner É. Lucas, it is stated that M. Mersenne (1644, 1647) implied that a necessary and sufficient condition for

- $2^p - 1$ *to be a prime is that* p *be a prime of one of the forms* $2^{2n} + 1$, $2^{2n} \pm 3$, *and* $2^{2n+1} - 1$.

Tanner expressed his belief and noted the sufficient condition would be false if $2^{67} - 1$ is composite.

There is also a missing restriction on the size of the prime because $2^3 - 1$ is prime, but 3 is not one of these forms.

So, there seems to be a belief that the exponents p of Mersenne primes have a special form.

If you check the numbers under 257, you will get Mersenne's list (except 3) plus the prime 61.

Sadly, the conditions quoted above are neither necessary nor sufficient. The Mersenne numbers M_p are composite for the following primes p: $257 = 2^8+1$, $1021 = 2^{10}-3$, $67 = 2^6+3$, and $8191 = 2^{13}-1$. So, none of the "sufficient" conditions hold.

Also, M_p is prime for $p = 89$, but 89 cannot be written in any of the listed forms.

3.1.5. P. T. Bateman, J. L. Selfridge, and Jr. S .S. Wagstaff presented (1989) the *new Mersenne conjecture.* It is as follows.

- *Let p be any odd positive integer. If two of the following conditions hold, then so does the third*:

1. $p = 2^k \pm 1$ or $p = 4^k \pm 3$;
2. $2^p - 1$ is a prime (a *Mersenne prime*);
3. $\frac{2^p+1}{3}$ is a prime (a *Wagstaff prime*).

This conjecture has been verified for all primes p less than 100000 and for all 51 known Mersenne primes. Some feel that "conjecture" is too strong of a word for the above and that perhaps this is even another case of *Guy's law of small numbers.*

3.1.6. As before, today, the Mersenne numbers give us most of the prime number records.

In 1811 P. Barlow wrote in his text, *Theory of Numbers*, that $2^{30}(2^{31}-1)$ "...is the greatest perfect number that will be discovered; for as they are merely curious, without being useful, it is not likely that any person will attempt to find one beyond it." Obviously, no one in the late 1800s had any idea of the power of modern computers.

After the 23rd Mersenne prime was found at the University of Illinois (Gilles, 1963), the Mathematics Department was so proud that the chair, Dr. Bateman, had their postage meter changed to stamp "$2^{11213} - 1$ is prime" on each envelope. This was used until the *four color theorem* was proved in 1976.

The 25th Mersenne prime was found by high-school students Laura Nickel and Landon Curt Noll (1978), who, though they had little understanding of the mathematics involved, used Lucas' simple test on the local university's mainframe.

D. Slowinski, who works for Cray computers, has written a version of the Lucas test that he has convinced many Cray labs around the world to run in their spare time. D. Slowinski does not search for record primes systematically. In fact, looking at the table of Mersenne primes, you can see that he missed the 29th prime but found the 30th (1983) and 31st (1985).

W. Colquitt and L. Welsh worked to fill in the gaps and found the 29th Mersenne prime in 1988.

Starting in late 1995, E. G. Woltman gathered up the disparate databases and combined them into one. Then, he placed this database and a free, highly optimized program to search for Mersenne primes onto the web. This started the Great Internet Mersenne Prime Search (GIMPS), which has now found the largest known Mersenne primes, combining the efforts of dozens of experts and thousands of amateurs.

Since 1997, all newly found Mersenne primes have been discovered by the GIMPS.

In late 1997, S. Kurowski (and others) established PrimeNet to automate the selection of ranges and reporting of results for GIMPS.

In 1999 (Hajratwala *et al.*), the first prime with more than 1000000 decimal digits (in fact, more than 2000000) was obtained. It is the 38th Mersenne prime, $M_{6972593}$; it has 2098960 decimal digits.

Let a *megaprime* be a prime number with at least one million decimal digits, then one can say that the first megaprime, $M_{6972593}$, was found in 1999.

Note, that the first "megaperfect" (i.e., perfect number with at least one million decimal digits) was obtained two years before in 1997. It has 1791864 digits and is of the form $194276\ldots 462976 = 2^{2976220}(2^{2976221}-1)$, corresponding to the 36th Mersenne prime $2^{2976221}-1$ with 895932 digits.

In 2018 (Laroche *et al.*), the last known (in fact, the 51st known) Mersenne prime, $M_{82589933}$, was obtained. It has 24862048 decimal digits.

So, as of 2021, 51 Mersenne primes as well as 51 (even) perfect numbers are known. In December 2020, a major milestone in the GIMPS project was passed after all exponents below 100 million were checked at least once.

List of known perfect numbers and Mersenne primes

	p	Number of digits in M_p	Number of digits in $2^{p-1}(2^p-1)$	Year	Discoverer
1	2	1	1	- - - -	- - - -
2	3	1	2	- - - -	- - - -
3	5	2	3	- - - -	- - - -
4	7	3	4	- - - -	- - - -
5	13	4	8	1456	anonymous
6	17	6	10	1588	Cataldi
7	19	6	12	1588	Cataldi
8	31	10	19	1772	Euler
9	61	19	37	1883	Pervushin
10	89	27	54	1911	Powers
11	107	33	65	1914	Powers
12	127	39	77	1876	Lucas
13	521	157	314	1952	Robinson
14	607	183	366	1952	Robinson
15	1279	386	770	1952	Robinson
16	2203	664	1327	1952	Robinson
17	2281	687	1373	1952	Robinson
18	3217	969	1937	1957	Riesel
19	4253	1281	2561	1961	Hurwitz
20	4423	1332	2663	1961	Hurwitz
21	9689	2917	5834	1963	Gillies
22	9941	2993	5985	1963	Gillies
23	11213	3376	6751	1963	Gillies
24	19937	6002	12003	1971	Tuckerman
25	21701	6533	13066	1978	Noll and Nickel
26	23209	6987	13973	1979	Noll
27	44497	13395	26790	1979	Nelson and Slowinski

(*Continued*)

(*Continued*)

	p	Number of digits in M_p	Number of digits in $2^{p-1}(2^p-1)$	Year	Discoverer
28	86243	25962	51924	1982	Slowinski
29	110503	33265	66530	1988	Colquitt and Welsh
30	132049	39751	79502	1983	Slowinski
31	216091	65050	130100	1985	Slowinski
32	756839	227832	455663	1992	Slowinski, Gage *et al.*
33	859433	258716	517430	1994	Slowinski and Gage
34	1257787	378632	757263	1996	Slowinski and Gage
35	1398269	420921	841842	1996	Armengaud, Woltman *et al.*
36	2976221	895932	1791864	1997	Spence, Woltman *et al.*
37	3021377	909526	1819050	1998	Clarkson, Woltman, Kurowski *et al.*
38	6972593	2098960	4197919	1999	Hajratwala, Woltman, Kurowski *et al.*
39	13466917	4053946	8107892	2001	Cameron, Woltman, Kurowski *et al.*
40	20996011	6320430	12640858	2003	Shafer, Woltman, Kurowski *et al.*
41	24036583	7235733	14471465	2004	Findley, Woltman, Kurowski *et al.*
42	25964951	7816230	15632458	2005	Nowak, Woltman, Kurowski *et al.*
43	30402457	9152052	18304103	2005	Cooper, Boone, Woltman, Kurowski *et al.*
44	32582657	9808358	19616714	2006	Cooper, Boone, Woltman, Kurowski *et al.*
45	37156667	11185272	22370543	2008	Elvenich, Woltman, Kurowski *et al.*
46	42643801	12837064	25674127	2009	Strindmo, Woltman, Kurowski *et al.*
47	43112609	12978189	25956377	2008	Smith, Woltman, Kurowski *et al.*
48 (?)	57885161	17425170	34850340	2013	Cooper, Woltman, Kurowski *et al.*
49 (?)	74207281	22338618	44677235	2016	Cooper, Woltman, Kurowski, Blosser *et al.*
50 (?)	77232917	23249425	46498850	2017	Pace, Woltman, Kurowski, Blosser *et al.*
51 (?)	82589933	24862048	49724095	2018	Laroche, Woltman, Blosser *et al.*

In the table above, we put question marks instead of a number for the last three Mersenne primes because it will not be known if there are other Mersennes in between these until a check and double check has been completed by GIMPS. See the GIMPS Status Page for more information. Not all smaller exponents have been tested.

3.1.7. Today, we can state that an exhaustive search by the GIMPS distributed computing project has shown that the first 48 even perfect numbers are

$$6,\ 28,\ 496,\ 8128,\ 33550336,\ 8589869056,\ 137438691328,\\ 2305843008139952128,\ 2658455991569831744654692615953842176,\\ \ldots,\ 169296\ldots130176$$

(sequence A000396 in the OEIS). They have the form $2^{p-1}(2^p - 1)$ for $p = 2$, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 42643801, 43112609, and 57885161 (sequence A000043 in the OEIS).

Three higher perfect numbers have also been discovered, namely those for which $p = 74207281$, 77232917, and 82589933, though there may be others within this range.

So, as of December 2021, 51 Mersenne primes, and, therefore, 51 even perfect numbers are known. The largest of them is $2^{82589932}$ $(2^{82589933} - 1)$ with 49724095 digits.

It has been conjectured that *there are infinitely many Mersenne primes.*

Although the truth of this conjecture remains unknown, it is equivalent, by the Euclid–Euler theorem, to the conjecture that *there are infinitely many even perfect numbers.*

3.1.8. However, it is also unknown whether there exists even a single odd perfect number.

In fact, odd perfect numbers either do not exist or are rare.

There are a number of results on perfect numbers that are actually quite easy to prove but nevertheless superficially impressive; some of them obviously come under Richard Guy's strong law of small numbers.

In 1496, Jacques Lefèvre stated that Euclid's rule gives all perfect numbers, thus implying that no odd perfect number exists.

Euler stated: "Whether ... there are any odd perfect numbers is a most difficult question." Euler proved that any odd perfect number has the form $q^{4\alpha+1}p_1^{2\beta_1} \cdot \ldots \cdot p_k^{2\beta_k}$, where $q, p_1, \ldots, p_k$ are distinct odd primes and $q \equiv \alpha \equiv 1 (mod\, 4)$.

More recently, Carl Pomerance has presented a heuristic argument suggesting that indeed no odd perfect number should exist.

All perfect numbers are also Ore's harmonic numbers, and it has been conjectured (Ore, 1948) as well that there are no odd Ore's harmonic numbers other than 1. So, if the *Ore's conjecture* is true, there are no odd perfect numbers.

Kanold, Tuckerman, Hagis, Stubblefield, Buxton, Elmore, Brent, Cohen, and te Riele have gradually pushed the bound to that there are no odd perfect number up to 10^{300}. To this day, it is known (Ochem and Rao, 2012) that there are no odd perfect numbers up to 10^{1500} [OcRa12].

In 1887, Sylvester conjectured and in 1925, Gradshtein proved that any odd perfect number must have at least six distinct prime factors. Hagis ans Chein have independently showed that an odd perfect number is divisible by at least eight distinct primes. Nielsen (2006) also showed that a general odd perfect number, if it exists, must have at least nine distinct prime factors.

Hagis and McDaniel show that the largest prime divisor is greater than 1001100, and Pomerance shows that the next largest is greater than 138.

Condict and Hagis have improved these bound to $3 \cdot 10^5$ and 10^3, respectively.

Now, it is proven that the largest three factors of an odd perfect number N must be at least 100000007, 10007, and 101.

Muskat proved that any odd perfect number is divisible by a prime power $> 10^{12}$. Ochem and Rao (2012) showed that the largest component of $N = q^{4\alpha+1}p_1^{2\beta_1} \cdot \ldots \cdot p_k^{2\beta_k}$ is greater than 10^{62}, i.e., either $q^{4\alpha+1} > 10^{62}$, or $p_j^{2\beta_j} > 10^{62}$ for some j.

Pomerance has also shown that an odd perfect number with at most k factors is less than $(4k)^{(4k)^{2^{k^2}}}$, and Heath-Brown has improved this by showing that if n is an odd number with k distinct prime factors, then $n < 4^{4^k}$. In 2003, Nielsen got the bound $n < 2^{4^{k+1}}$.

For additional information, see, for example, [DeKo18], [Dick05], [Nank79], [Ore48], [Salo90], [Sier64], [OcRa12], [Wiki22], [Deza17], [Deza18], [Prim22], and [Yan96].

3.2. Divisor Function and Perfect Numbers

Definition of perfect numbers and divisor functions

3.2.1. A *perfect number* is a positive integer that is equal to the sum of its proper divisors, i.e., positive integer divisors, excluding the number itself.

The sum of positive integer divisors of a number n, excluding the number itself, is called its *aliquot sum*; so, a perfect number is one that is equal to its aliquot sum.

In terms of the *aliquot sum function* (or *restricted divisor function*)

$$s(n) = \sum_{d|n,\ d\neq n} d,\ \in \mathbb{N},$$

giving the sum of all proper divisors of a positive integer n, i.e., all positive integer divisors of n other than n itself, the classical definition of a perfect number n takes the form

$$s(n) = n.$$

For instance, the number 6 has three proper divisors 1, 2, and 3, and $s(6) = 1+2+3 = 6$, so 6 is a perfect number. The number 28 has five proper divisors 1, 2, 4, 7, and 14, and $s(28) = 1+2+4+7+14 = 28$, so 28 is a perfect number. Similarly, the number 496 has nine proper divisors 1, 2, 4, 8, 16, 31, 62, 124, and 238; it is perfect, as

$s(496) = 1+2+4+8+16+31+62+124+248 = 496$. The number 8128 has 13 proper divisors 1, 2, 4, 8, 16, 32, 64, 127, 254, 508, 1016, 2032, and 4064; it is perfect, as $s(8128) = 1+2+4+8+16+32+64+127+254+508+1016+2032+4064 = 8128$.

While the ancient Greeks originally defined perfect numbers in terms of the sum of the proper divisors, it is more convenient for most purposes to define a positive integer n as perfect if n satisfies the condition

$$\sigma(n) = 2n,$$

where

$$\sigma(n) = \sum_{d|n} d, \ \ n \in \mathbb{N},$$

is the sum of divisors function, giving the sum of all positive integer divisors of a positive integer n, including n itself.

For instance, the number 6 has four positive integer divisors 1, 2, 3, and 6, and $\sigma(6) = s(6+6) = 1+2+3+6 = 12 = 2\cdot 6$, so 6 is a perfect number. The number 28 has 6 positive integer divisors 1, 2, 4, 7, 14, and 28, and $\sigma(28) = s(28)+28 = 1+2+4+7+14+28 = 56 = 2\cdot 28$, so 28 is a perfect number. Similarly, the number 496 is perfect, as $\sigma(496) = s(496)+496 = 1+2+4+8+16+31+62+124+248+496 = 992 = 2\cdot 496$, as well as the number 8128, for which $\sigma(8128) = s(8128)+8128 = 1+2+4+8+16+32+64+127+254+508+1016+2032+4064+8128 = 16256 = 2\cdot 8128$.

In other words, a perfect number is a number that is half of the sum of all its positive divisors including itself.

Much of the study of perfect numbers relies on the fact that $\sigma(n)$ is a multiplicative function.

3.2.2. The various sums of divisors give various kinds of numbers.

Numbers where the sum of the proper divisors is less than the number itself are called *deficient*. For a deficient number, it holds that $s(n) < n$ or, equivalently, $\sigma(n) < 2n$.

For instance, the number 4 is deficient, as it has two proper divisors, 1 and 2, and $s(4) = 1+2 < 4$. Equivalently, $\sigma(4) = 1+2+4 = 7 < 2\cdot 4$.

The first few deficient numbers are 1, 2, 3, 4, 5, 7, 8, 9, 10, 11,... (sequence A005100 in the OEIS).

Numbers where the sum of the proper divisors is greater than the number itself are called *abundant*. For an abundant number, it holds that $s(n) > n$ or, equivalently, $\sigma(n) > 2n$.

For instance, the number 12 is abundant, as it has five proper divisors 1, 2, 3, 4, 6, and $s(12) = 1 + 2 + 3 + 4 + 6 = 16 > 12$. Equivalently, $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28 > 2 \cdot 12$.

The first few abundant numbers are 12, 18, 20, 24, 30, 36, 40, 42, 48, 54,... (sequence A005101 in the OEIS).

So, any positive integer is a deficient, an abundant, or a perfect number. Terms *deficient* and *abundant*, together with the term *perfect* itself, come from Greek numerology.

A pair of numbers which are the sum of each other's proper divisors are called *amicable*. For such a pair (m, n), it holds that

$$s(n) = m, \ s(m) = n,$$

or, equivalently,

$$\sigma(n) = \sigma(m) = n + m.$$

For instance, the pair $(220, 284)$ is an amicable pair. In fact, the number 220 has 11 proper divisors 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, and 110, whose sum is 284; so, $s(220) = 284$. The number 284 has five proper divisors 1, 2, 4, 71, and 142, whose sum is 220; so, $s(284) = 220$. Equivalently, $\sigma(220) = s(220)+220 = 284+220 = 504$, while $\sigma(284) = s(284) + 284 = 220 + 284 = 504$.

The first few amicable pairs are (220, 284), (1184, 1210), (2620, 2924), (5020, 5564), (6232, 6368), (10744, 10856), (12285, 14595), (17296, 18416), (63020, 76084), (66928, 66992),... (sequence A259180 in the OEIS; see also A002025 and A002046).

The larger cycles of numbers are called *sociable*. For instance, we get a *sociable quadruple* (or *sociable 4-cycle*, *amicable 4-cycle*) (n_1, n_2, n_3, n_4) if

$$s(n_1) = n_2, \ s(n_2) = n_3, \ s(n_3) = n_4, \ \text{and } s(n_4) = n_1.$$

Equivalently, in terms of sigma function, it holds that

$$\sigma(n_1) = n_1 + n_2,\ \sigma(n_2) = n_2 + n_3,\ \sigma(n_3) = n_3 + n_4, \text{ and}$$

$$\sigma(n_4) = n_4 + n_1.$$

For instance, the quadruple (1264460, 1547860, 17276361305184) gives an example of amicable 4-cycle.

In fact, the sum $s(1264460)$ of the proper divisors of $1264460 = 2^2 \cdot 5 \cdot 17 \cdot 3719$ is

$$1 + 2 + 4 + 5 + 10 + 17 + 20 + 34 + 68 + 85 + 170 + 340 + 3719 + 7438 + 14876 + 18595 + 37190 + 63223 + 74380 + 126446 + 252892 + 316115 + 632230 = 1547860;$$

the sum $s(1547860)$ of the proper divisors of $1547860 = 2^2 \cdot 5 \cdot 193 \cdot 401 = 2^2 \cdot 5 \cdot 193 \cdot 401$ is

$$1 + 2 + 4 + 5 + 10 + 20 + 193 + 386 + 401 + 772 + 802 + 965 + 1604 + 1930 + 2005 + 3860 + 4010 + 8020 + 77393 + 154786 + 309572 + 386965 + 773930 = 1727636;$$

the sum $s(1727636)$ of the proper divisors of $1727636 = 2^2 \cdot 521 \cdot 829 = 2^2 \cdot 521 \cdot 829$ is

$$1 + 2 + 4 + 521 + 829 + 1042 + 1658 + 2084 + 3316 + 431909 + 863818 = 1305184;$$

finally, the sum $s(1305184)$ of the proper divisors of $1305184 = 2^5 \cdot 40787 = 2^5 \cdot 40787$ is

$$1 + 2 + 4 + 8 + 16 + 32 + 40787 + 81574 + 163148 + 326296 + 652592 = 1264460.$$

It is easy to see that sociable numbers give a generalization of amicable numbers, while perfect numbers can be considered as a particular case of amicable pairs with two equal elements: a perfect number n is amicable to itself, as it holds that $s(n) = n$.

Using other approaches, we can get many interesting classes of special numbers (*multiply perfect*, *quasiperfect*, *almost perfect*, etc.), which are closely connected with perfect numbers and having arithmetical properties, depending on the structure of their positive integer divisors.

We consider many such classes of numbers in Section 3.5 of this chapter and, especially, in Chapter 5.

Even perfect numbers and Euclid–Euler theorem

3.2.3. The set of even perfect numbers is completely characterized by the *Euclid–Euler theorem*, partially proved by Euclid and completed by Euler.

Theorem (Euclid–Euler theorem). *An even natural number is perfect if and only if* $n = 2^{k-1}(2^k - 1)$, *where* $2^k - 1 \in P$.

Prime numbers of the form $2^k - 1$ are known as *Mersenne primes*. They are prime elements in the sequence 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047,... of Mersenne numbers (sequence A000225 in OEIS).

In fact, a *Mersenne number* is a positive integer of the form

$$M_k = 2^k - 1, \; k \in \mathbb{N}.$$

For $2^k - 1$ to be prime, it is necessary that k itself be prime. By this reason, many authors require that the exponent k in the definition above be a prime.

Mersenne numbers $M_p = 2^p - 1$ with prime p form the sequence 3, 7, 31, 127, 2047, 8191, 131071, 524287, 8388607, 536870911,... (sequence A001348 in OEIS).

In fact, the exponents k which give Mersenne primes are 2, 3, 5, 7, 13, 17, 19, 31,... (sequence A000043 in the OEIS), and the resulting Mersenne primes are 3, 7, 31, 127, 8191, 131071, 524287, 2147483647,... (sequence A000668 in the OEIS).

This class of special numbers is of great interest because the *Mersenne primes* (prime Mersenne numbers) are among the oldest and most studied of all primes.

In fact, Mersenne primes are very rare: Not all numbers of the form $2^p - 1$ with a prime p are primes; for example,

$$2^{11} - 1 = 2047 = 23 \cdot 89$$

is not a prime number.

For instance, for the 2610944 prime numbers p up to 43112609, the corresponding Mersenne numbers $M_p = 2^p - 1$ is prime for only 47 of them. Today, we know only 51 Mersenne primes.

The frequency of Mersenne primes is the subject of the *Lenstra–Pomerance–Wagstaff conjecture*, which states that

- *the expected number of Mersenne primes less than some given x is*
$$\frac{e^\gamma}{\log 2} \cdot \log\log x,$$
where $\gamma = 0.5772156649\ldots$ is the Euler–Mascheroni constant.

3.2.4. So, we obtain a new even perfect number if and only if we obtain a new Mersenne prime:

- *The nth even perfect number has the form $n = 2^{p-1}M_p$, where $M_p = 2^p - 1$ is the nth Mersenne prime.*

As of 2021, there exist 51 known Mersenne primes. It means that there exists 51 known (even) perfect numbers. The four smallest perfect numbers are

$$6 = 2^1(2^2 - 1) = 2 \cdot M_2;\ 28 = 2^2(2^3 - 1) = 2^2 \cdot M_3;$$
$$496 = 2^4(2^5 - 1) = 2^4 \cdot M_5;\ 8128 = 2^6(2^7 - 1) - 2^6 \cdot M_7.$$

The four biggest known perfect numbers are

$$2^{57885160}(2^{57885161} - 1) = 2^{257885160} \cdot M_{57885161}(34850339 \text{ digits});$$
$$2^{74207280}(2^{74207281} - 1) = 2^{74207280} \cdot M_{274207281}(44677235 \text{ digits});$$
$$2^{77232916}(2^{77232917} - 1) = 2^{77232916} \cdot M_{277232917}(46498850 \text{ digits});$$
$$2^{82589932}(2^{82589933} - 1) = 2^{82589932} \cdot M_{282589933}(49724095 \text{ digits}).$$

While $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127, \ldots, M_{57885161} = 581887\ldots285951$ (17425170 digits) are first, second, third, fourth, …, 48th Mersenne primes, for the last three known Mersenne primes, $M_{274207281}$, $M_{277232917}$, $M_{282589933}$, the ranking is still provisional. It has not been verified whether any undiscovered Mersenne primes exist between the 48th ($M_{57885161}$) and the 51st known ($M_{82,589,933}$) Mersenne primes.

Proof of the Euclid-Euler theorem

3.2.5. As was considered before, a perfect number is a number that is half the sum of all of its positive divisors including itself; in symbols,

$$\sigma(n) = 2n, \quad \text{where} \;\; \sigma(n) = \sum_{d|n} d.$$

The proof of the *Euclid–Euler theorem* depends on the fact that the *sum of divisors function* $\sigma(n)$ is multiplicative; that is, if a and b are any two relatively prime integers, then

$$\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b).$$

For this formula to be valid, the sum of divisors of a number must include the number itself, not just the proper divisors.

3.2.6. Consider the Euclid's part of the theorem (sufficiency):

- *Any number* $2^{k-1}(2^k - 1)$ *with a prime number* $2^k - 1$ *is a perfect number.*

□ The part already proved by Euclid immediately follows from the multiplicative property: Every Mersenne prime gives rise to an even perfect number. When $2^p - 1$ is prime,

$$\sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\sigma(2^p - 1).$$

The divisors of 2^{p-1} are $1, 2, 4, 8, \ldots, 2^{p-1}$. The sum of these divisors is a geometric series whose sum is $2^p - 1$.

Next, since $2^p - 1$ is prime, its only divisors are 1 and itself, so the sum of its divisors is 2^p.

Combining these, we get

$$\begin{aligned}\sigma(n) = \sigma(2^{p-1}(2^p - 1)) &= \sigma(2^{p-1})\sigma(2^p - 1)\\ &= (2^p - 1)(2^p)\\ &= 2(2^{p-1})(2^p - 1) = 2n.\end{aligned}$$

Therefore, $2^{p-1}(2p - 1)$ is perfect. □

3.2.7. Consider the Euler's part of the theorem (necessity):

- *If n is an even perfect number, then it has the form $n = 2^{k-1}(2^k - 1)$, where $2^k - 1 \in P$.*

□ In this direction, suppose that an even perfect number has been given, we partially factor it as $2^k x$, where x is odd.

For $2^k x$ to be perfect, the sum of its divisors must be twice its value:

$$2^{k+1}x = \sigma(2^k x) = (2^{k+1} - 1)\sigma(x).$$

The odd factor $2^{k+1} - 1$ on the right-hand side is at least 3, and it must divide x, the only odd factor on the left-hand side, so $y = \frac{x}{2^{k+1}-1}$ is a proper divisor of x:

$$x = (2^{k+1} - 1)y.$$

The factor 2^{k+1} on the left-hand side must divide $\sigma(x)$, the only even factor on the right-hand side, so

$$y = \frac{\sigma(x)}{2^{k+1}}$$

is a proper divisor of $\sigma(x)$:

$$\sigma(x) = 2^{k+1}y.$$

Dividing both sides by the common factor $2^{k+1} - 1$ gives

$$2^{k+1}y = \sigma(x).$$

Taking into account the known divisors $x = (2^{k+1} - 1)y$ and y of x gives

$$\sigma(x) \geq y + x = y + (2^{k+1} - 1)y.$$

For the above equality to be true, there can be no other divisors of x. Therefore, y must be 1, and x must be a prime of the form $2^{k+1} - 1$. □

For some additional information, see, for example, in [Buch09], [DeKo13], [Deza17], [Deza18], [Dick05], [Sier64], [Step01], [Deza21], and [Yan96].

Mystery of odd perfect numbers

> *Whether ... there are any odd perfect numbers is a most difficult question.*
>
> — Euler
>
> *... a prolonged meditation on the subject has satisfied me that the existence of any one such (odd perfect number) - its escape, so to say, from the complex web of conditions which hem it in on all sides—would be little short of a miracle.*
>
> — Sylvester

3.2.8. As for odd perfect numbers, mathematicians cannot find one. If odd perfect numbers exist, they should be very large and very special.

Though it is unknown whether any odd perfect numbers exist, various results have been obtained.

For example, any odd perfect number N must satisfy the following conditions:

- N is a perfect square times an odd power of a single prime;
- N is divisible by at least nine primes and has at least 75 prime factors, not necessarily distinct (more precisely, N has at least 12 distinct prime factors if it is not divisible by 3, at least 15 distinct prime factors if it is not divisible by 3 and by 5, and at least 27 distinct prime factors if it is not divisible by 3, by 5, and by 7);
- N has at least 1500 decimal digits, i.e., $N > 10^{1500}$;
- N has a prime divisor greater than 10^8;
- N has a prime divisor less than $e^{4.97401\cdot 10^{10}}$;
- $N < 2^{4^{k+1}}$, where $k+1$ is the number of distinct prime factors of N;
- N is of the form $N \equiv 1 (mod\ 12)$ or $N \equiv 9 (mod\ 36)$.

In fact, Euler proved that any odd perfect number has the form

$$q^{4\alpha+1} p_1^{2\beta_1} \cdot \ldots \cdot p_k^{2\beta_k},$$

where $q, p_1, \ldots, p_k$ are distinct odd primes and $q \equiv \alpha \equiv 1 (mod\ 4)$.

3.2.9. Consider more exactly some results connected with the number of prime divisors of an odd perfect number N.

In 1887, Sylvester conjectured and in 1925, Gradshtein proved that

- *any odd perfect number must have at least six distinct prime factors.*

Hagis (1980) showed that

- *any odd perfect number must have at least eight distinct prime factors, in which case the number is divisible by* 15.

In 1888, Catalan proved that

- *if an odd perfect number is not divisible by* 3*,* 5*, or* 7*, it has at least* 26 *distinct prime aliquot factors.*

This amount was extended to 27 by Norton (1960). Norton (1960) also showed that

- *odd perfect numbers not divisible by* 3 *or* 5 *must have at least* 15 *distinct prime factors.*

Neilsen (2006), improving the bound of Hagis (1980), showed that

- *if an odd perfect number is not divisible by* 3*, it must have at least* 12 *distinct prime factors.*

Nielsen (2006) also showed that

- *any odd perfect number must have at least nine distinct prime factors.*

More recently, Hare (2005) has shown that

- *any odd perfect number must have at least* 75 *prime factors.*

Ochem and Rao (2012) subsequently showed that

- *any odd perfect number has at least* 101 *not necessarily distinct prime factors.*

Moreover, Nielsen (2015) proved that

- *any odd perfect number has at least* 10 *distinct prime factors.*

3.2.10. To this day, it is not known that if any odd perfect numbers exist, although numbers up to 10^{1500} have been checked without success. The following table summarizes the development of ever-higher bounds for the smallest possible odd perfect number.

Author	Bound
Kanold (1957)	10^{20}
Tuckerman (1973)	10^{36}
Hagis (1973)	10^{50}
Brent and Cohen (1989)	10^{160}
Brent *et al.* (1991)	10^{300}
Ochem and Rao (2012)	10^{1500}

3.2.11. For the largest prime factor of an odd perfect number N, Iannucci (1999, 2000) and Jenkins (2003) were able to find lower bounds.

It is proven that

- *the largest prime factor of N is greater than 10^8, the second largest prime factor is greater than 10^4, and the third largest prime factor is greater than 10^2.*

Therefore,

- *the largest three factors of an odd perfect number N must be at least* 100000007, 10007, *and* 101.

Goto and Ohno (2006) verified that the largest factor must be at least 100000007 using an extension to the methods of Jenkins.

Ochem and Rao (2012) subsequently showed that

- *the largest component of $N = q^{4\alpha+1}p_1^{2\beta_1} \cdot \ldots \cdot p_k^{2\beta_k}$ is greater than 10^{62}, i.e., either $q^{4\alpha+1} > 10^{62}$ or $p_j^{2\beta_j} > 10^{62}$ for some j.*

On the other hand (Yamada, 2005), it is proven that

- *the smallest prime factor of an odd perfect number N with all even powers lower than six must be less than $e^{4.97401 \cdot 10^{10}}$.*

3.2.12. Pomerance has also shown that

- *an odd perfect number with at most* k *factors is less than* $(4k)^{(4k)^{2^{k^2}}}$.

Heath-Brown has improved this by showing that *if* n *is an odd number with* $\sigma(n) = an$, *then* $n < (4d)^{4^k}$, *where* d *is the denominator of* a, *and* k *is the number of distinct prime factors of* n. In particular,

- *if* n *is an odd perfect number with* k *distinct prime factors, then* $n < 4^{4^k}$.

Moreover (Nielsen, 2003),

- *if* $N = q^{4\alpha+1}p_1^{2\beta_1} \cdot \ldots \cdot p_k^{2\beta_k}$ *is an odd perfect number, then* $N < 2^{4^{k+1}}$.

In fact, it was proven by Chen and Tang (2014) that $N < 2^{(4^{k+1}-2^{k+1})}$.

3.2.13. It was proven by Tuchard (1953) and Holdeber (2003) that N must be equal to 1 modulo 12 or 9 modulo 36. To be more precise, it can be shown (Roberts, 2008) that

- *any odd perfect number* N *is of the form* $N \equiv 1(mod\ 12)$, *or* $N \equiv 117(mod\ 468)$, *or* $N \equiv 81(mod\ 324)$.

3.2.14. Furthermore, several minor results are known about the exponents $\beta_1, \ldots, \beta_k$ in the representation $N = q^{4\alpha+1}p_1^{2\beta_1} \cdot \ldots \cdot p_k^{2\beta_k}$ of an odd perfect number. In fact,

- *if* $\beta_1 = \beta_2 = \cdots = \beta_k = \beta$, *then for a given* β, *there exist only finite number of odd perfect numbers.*

In particular, for β equal to 1, 2, 3, 5, 6, 8, 11, 12, 17, 24, or 62, there are no odd perfect numbers (see [HaMc72], [McHa75], and [CoWi85]).

Moreover, in this case, it holds that $N < 2^{4^{2\beta^2+8\beta+3}}$ (Yamada, 2019).

Similarly (Kanold, 1950; Cohen and Williams, 1985), it holds that

- $(\beta_1, \ldots, \beta_k) \neq (1, \ldots, 1, 3)$, $(\beta_1, \ldots, \beta_k) \neq (1, \ldots, 1, 5)$, *and* $(\beta_1, \ldots, \beta_k) \neq (1, \ldots, 1, 6)$.

It is proven also that not all $\beta_i \equiv 1(mod\ 3)$ (McDaniel, 1970), as well as not all $\beta_i \equiv 2(mod\ 5)$ (Fletcher *et al.*, 2012).

3.2.15. Many of the properties proved about odd perfect numbers also apply to *Descartes numbers*, and Pace Nielsen has suggested that sufficient study of those numbers may lead to a proof that no odd perfect numbers exist (see Section 3.6 of this Chapter).

For more information, see [Ribe96], [Guy94], [Niel03], [PoLu10], [FNO12], [HaMc72], [Robe08], [CoWi85], [Yama19], [Cohe87], [McDa70], [FNO12], [Deza21], [Deza17], [Dick05], [Yan96], and [Niel07].

Exercises

1. Prove that odd perfect number cannot be a perfect square.
2. Consider the numbers $2^{n-1}(2^n - 1)$ for all positive integers n. Find all perfect numbers of this form with $n \leq 15$. Are there deficient numbers of this form? Are there abundant numbers of this form?
3. Consider the numbers $2^\alpha(2^\beta + 1)$ and $2^\beta + 1 \in P$, with positive integers α and β. Find all perfect numbers of this form. Are there deficient numbers of this form? Are there abundant numbers of this form?
4. Prove that there are infinitely many deficient numbers.
5. Prove that there are infinitely many abundant numbers.
6. Find all n such that $\tau(n) = 2n$; $2\tau(n) = n$; $\tau(n) = n$; $\sigma(n) = n$.
7. Are there $n \leq 100$ such that $\sigma_2(n) = \sum_{d|n} d^2 = 2n^2$?
8. Find all perfect numbers n such that $\sigma(n)$ is perfect; such that $\sigma(\sigma(n))$ is perfect.
9. Does there exist perfect numbers equal to a^3, $a \in \mathbb{N}$?
10. Check if only one known perfect number (28) has the form $x^3 - 1$.

3.3. Properties of Perfect Numbers

All even perfect numbers have a very precise form; odd perfect numbers either do not exist or are rare. There are a number of results on perfect numbers that are actually quite easy to prove but nevertheless very impressive.

In this section, we give a large list of the simplest properties of perfect numbers. All of them can be proven using elementary properties of divisibility of integers.

Historical tricks in the theory of perfect numbers

3.3.1. The first four perfect numbers, 6, 278, 496, and 8128, were the only ones known to early Greek mathematics. Studying the properties of these four numbers, ancient mathematicians made some general assumptions. Most of them turned out to be false.

Euclid proved that $2^{p-1}(2^p-1)$ is an even perfect number whenever 2^p-1 is prime (*Elements*, Prop. IX.36).

Obviously, the first four perfect numbers are obtained by using the formula above the first four primes $2, 3, 5$, and 7:

for $p=2$, we get $2^1(2^2-1)=2\cdot 3=6$;
for $p=3$, we get $2^2(2^3-1)=4\cdot 7=28$;
for $p=5$, we get $2^4(2^5-1)=16\cdot 31=496$;
for $p=7$, we get $2^6(2^7-1)=64\cdot 127=8128$.

It is natural to propose that

- *the kth perfect number can be obtained by using the Euclid's formula $2^{p-1}(2^p-1)$ with $p=p_k$, where p_k is the kth prime number.*

But now, we know that there are composite Mersenne numbers with prime indexes. The first such number is $M_{11}=2^{11}-1=23\cdot 89$.

The next are 23, 29, 37, 41, 43, 53, 59, 67, 71, 73, ... (sequence A054723 in the OEIS).

So, already the next prime $p = 11$ gives us an counterexample to the conjecture above, and after three "good" primes, 13, 17, and 19, we obtain the next two counterexamples for the primes, 23 and 29.

As the first perfect number has one decimal digit, the second perfect number has two decimal digits, the third perfect number has three decimal digits, and the fourth perfect number has four decimal digits, it is easy to conjecture that

- *the kth perfect number has exactly k decimal digits.*

However, it turns out that the fifth perfect number $33550336 = 2^{12}(2^{13} - 1)$ has eight decimal digits.

Lastly, the first four perfect numbers 6, 278, 496, and 8128 end in 6 and 8; moreover, they end in 6 and 8 alternatively. So, one can conjecture that

- *all the perfect numbers end in* 6 *and* 8 *alternatively.*

In fact, the fifth perfect number $33550336 = 2^{12}(2^{13} - 1)$ really ends in 6. However, the sixth perfect number $8589869056 = 2^{16}(2^{17} - 1)$ also end by 6, and therefore, the conjecture above is false.

On the other hand, it is easy to prove that the last digit of any even perfect number is 6 or 8. We consider this fact later. It is easy to check that the sequence of the last digits of even perfect numbers starts from elements 6, 8, 6, 8, 6, 6, 8, 8, 6, 6, 8, 8, 6, 8, 8, ... (sequence A094540 in the OEIS).

One more conjecture by ancient mathematicians is still open. In fact, in 1496, Jacques Lefèvre stated that Euclid's rule gives all perfect numbers, thus implying that

- *no odd perfect number exists.*

In fact, it is still unknown whether odd perfect numbers exist or not.

Primality of $2^n - 1$ and properties of perfect numbers

3.3.2. First of all, consider elementary properties of even perfect numbers $2^{n-1}(2^n - 1)$, connected with the primality of the number $2^n - 1$.

It is easy to see that a number of the form $2^n - 1$ can be a prime only if n is a prime:

- *For a positive integer* n, *if* $2^n - 1 \in P$, *then* $n \in P$.

□ In fact, consider $n \in \mathbb{N}$. If $n = 1$, one has $2^1 - 1 = 1$; it is not a prime. If n is composite, one can find positive integers a and b such that $n = a \cdot b$ and $1 < a \leq b < n$. Then,

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a) - 1) \cdot K, \ K \in \mathbb{N}.$$

So, the number $2^n - 1$ has a positive integer divisor $2^a - 1$. As $1 < a < n$, it holds that $1 < 2^a - 1 < 2^n - 1$. It means that $2^a - 1 \neq 1$ is a proper divisor of $2^n - 1$; so, $2^n - 1$ is composite. □

As a consequence, we get the following elementary fact:

- *For a positive integer* n, *if* $n \in S$, *then* $2^n - 1 \in S$.

However, there exist primes p such that $2^p - 1$ is composite. The first such number is 11:

$$M_{11} = 2^{11} - 1 = 1027 = 23 \cdot 89.$$

The next are 23, 29, 37, 41, 43, 53, 59, 67, 71, 73, ... (sequence A054723 in the OEIS).

As an easy subsequence of the fact above, we can state that

- *any even perfect number has the form* $2^{p-1}(2^p - 1)$, *where* $p \in P$.

For any even perfect number greater than 6, the corresponding prime number p is odd, and hence, the number $p - 1$ is even. So, the following proposition holds:

Any even perfect number greater than 6 *is divisible by* 4.

□ As for any prime number $p \neq 2$, it holds that $p - 1 \geq 2$; we get $2^{p-1} \geq 2^2$, so $4|2^{p-1}$ and $4|2^{p-1}(2^p - 1)$. □

Moreover, it is easy to state that

- *the only square-free perfect number is* 6.

□ For even perfect numbers, it is now obvious. As for odd perfect numbers, it is proven that any odd perfect number has the form $q^{\alpha}p_1^{2\alpha_1}\cdots p_k^{2\alpha_k}$, where $q, p_1, \ldots, p_k$ are distinct odd primes (Euler). So, the proposition is true for all, even and odd, perfect numbers. □

Moreover, it is easy to check that *greatest common divisor of two even perfect numbers is a power of two.* More exactly,

- *for two given even perfect numbers* $2^{p-1}(2^p - 1)$ *and* $2^{q-1}(2^q - 1)$, $p, q \in P, p < q$, *their greatest common divisor is equal to* 2^{p-1}.

□ In fact, for two even perfect numbers $2^{p-1}(2^p - 1)$ and $2^{q-1}(2^q - 1)$, it holds that $2^p - 1, 2^q - 1 \in P \backslash \{2\}$, and for $p < q$, we get

$$gcd(2^{q-1}(2^q - 1), 2^{p-1}(2^p - 1)) = 2^{p-1}. \qquad \square$$

In other words, the greatest common divisor of these two perfect numbers is $\frac{M_p+1}{2}$, where M_p is the Mersenne prime, taking part in the construction of the smaller perfect number. In particular, if both perfect numbers are greater than 3, then $p - 1$ is even, and hence, the greatest common divisor of these two perfect numbers is greater than 4.

3.3.3. Consider now possible remainders of Mersenne primes modulo 10. It will give us information about the last digit of the prime Mersenne number M_p. In fact, as any odd prime number p is congruent to 1 or 3 modulo 4, we have the following proposition:

- *for* $p = 2$, *it holds that* $M_p \equiv 3(mod\ 10)$, *i.e., the last digit of* M_2 *is* 3;
- *for* $p \in P$, $p = 4l + 1$, *it holds that* $M_p \equiv 1(mod\ 10)$, *i.e., the last digit of* M_p *is* 1;
- *for* $p \in P$, $p = 4l + 3$, *it holds that* $M_n \equiv 7(mod\ 10)$, *i.e., the last digit of* M_p *is* 7.

□ The reader can easily check these facts, noting that

$$2^{4l+k} - 1 \equiv (2^4)^l \cdot 2^k - 1 \equiv 6^l \cdot 2^k - 1 \equiv 6 \cdot 2^k - 1 (mod\ 10);$$

as $6 \cdot 2^1 - 1 \equiv 1 (mod\ 10)$, $6 \cdot 2^2 - 1 \equiv 3 (mod\ 10)$, and $6 \cdot 2^3 - 1 \equiv 7 (mod\ 10)$, the result holds. □

Considering now a given even perfect number, we can get the following simple fact:

- *for* $p = 2$, *it holds that* $2^{p-1} \equiv 2 (mod\ 10)$, *and* $2^p - 1 \equiv 3 (mod\ 10)$;
- *for* $p \in P$, $p = 4l + 1$, *it holds that* $2^{p-1} \equiv 6 (mod\ 10)$, *and* $2^p - 1 \equiv 1 (mod\ 10)$;
- *for* $p \in P$, $p = 4l + 3$, *it holds that* $2^{p-1} \equiv 4 (mod\ 10)$, *and* $2^p - 1 \equiv 7 (mod\ 10)$.

□ Really, it is easy to see that

$$2^{4l+k} \equiv (2^4)^l \cdot 2^k \equiv 6^l \cdot 2^k \equiv 6 \cdot 2^k (mod\ 10);$$

as $6 \cdot 2^1 \equiv 2 (mod\ 10)$, $6 \cdot 2^0 \equiv 6 (mod\ 10)$, and $6 \cdot 2^2 - 1 \equiv 4 (mod\ 10)$, the result holds. □

We use this fact in the next section.

Modular properties

In the previous section, we also started to discuss some properties of even perfect numbers modulo n, $n \in \mathbb{N}$.

Let us consider such kind of properties in detail.

3.3.4. As for modulo 2, we can state that

- *any even perfect number is congruent to* 0 *modulo* 2.

Moreover, it holds that

- *any even perfect number greater than* 6 *is congruent to* 0 *modulo* 4.

□ Both these facts are trivial: $2^{p-1} \equiv 0 (mod\ 2)$ for any prime p, while $2^{p-1} \equiv 0 (mod\ 4)$ for any prime $p > 2$. □

In a similar way, we can prove that

- *any even perfect number greater than* 6 *is congruent to* 4 *modulo* 6.

□ In fact, for odd p, it holds that

$$2^{p-1}(2^p - 1) \equiv (-1)^{p-1}((-1)^p - 1) \equiv 1 \cdot (-2) \equiv 1(mod\ 3);$$

so, $2^{p-1}(2^p-1) \equiv 1(mod\ 3)$, i.e., $2^{p-1}(2^p-1) = 3t+1$. Since $2^{p-1}(2^p-1) \equiv 0(mod\ 2)$, we get $3t + 1 \equiv 0(mod\ 2)$, and $t \equiv 1(mod\ 2)$. So, $t = 2m + 1$, and $2^{p-1}(2^p - 1) = 3t + 1 = 3(2m + 1) + 1 = 6m + 4$. Therefore, $2^{p-1}(2^p - 1) \equiv 4(mod\ 6)$. □

3.3.5. If we consider modulo 10, we get that *any even perfect number is congruent to* 6 *or* 8 *modulo* 10:

- *If* $n = 2^{k-1}(2^k - 1)$, *where* $2^k - 1 \in P$, *then* $n \equiv 6, 8(mod\ 10)$.

In other words, it is easy to show that *the last digit of any even perfect number is* 6 *or* 8.

□ In fact, consider the numbers $2^{p-1}(2^p - 1)$. For $p = 2$, the statement is true:

$$2^1(2^2 - 1) \equiv 2 \cdot 3 \equiv 6(mod\ 10).$$

All other p are odd (as p is prime) and hence $p \equiv 1, 3(mod\ 4)$. If $p \equiv 1(mod\ 4)$, then $p = 4l + 1$ and

$$2^{p-1}(2^p - 1) \equiv (2^4)^l(2(2^4)^l - 1) \equiv 6(12 - 1) \equiv 6(mod\ 10).$$

If $p \equiv 3(mod\ 4)$, then $p = 4l + 3$ and

$$2^{p-1}(2^p - 1) \equiv 4(2^4)^l(8(2^4)^l - 1) \equiv 24(48 - 1) \equiv 4 \cdot 7 \equiv 8(mod\ 10).$$

On the other hand, we can easily obtain this result using the information about the last digit of a given Mersenne prime $M_p > 3$ proved in the previous section: If $M_p = 2^p - 1 \equiv 1(mod\ 10)$, then $2^{p-1} \equiv 6(mod\ 10)$, and $2^{p-1}(2^p - 1) \equiv 6(mod\ 10)$; if $M_p = 2^p - 1 \equiv 7(mod\ 10)$, then $2^{p-1} \equiv 4(mod\ 10)$, and $2^{p-1}(2^p - 1) \equiv 4 \cdot 7 \equiv 8(mod\ 10)$. □

It is easy to check that the sequence of the last digits of even perfect numbers starts from elements 6, 8, 6, 8, 6, 6, 8, 8, 6, 6, 8, 8, 6, 8, 8,. . . (sequence A094540 in the OEIS).

Similarly, *the last two digits of any even perfect number greater than* 6 *are* 16, 28, 36, 56, 76, *or* 96:

- *If* $n = 2^{k-1}(2^k - 1)$, *where* $2^k - 1 \in P\backslash\{2\}$, *then* $n \equiv 16, 28, 36, 56, 76 (mod\ 100)$.

Note that there is only one combination, “28,” with the last digit 8, while one has four possibilities, “16, 36, 56, and 76,” with the last digit 6. So, one can say that

- *any even perfect numbers ends by* 6 *or* 28.

3.3.6. Consider now the behavior of even perfect numbers modulo 9. It is easy to prove that

- *any even perfect number greater than* 6 *gives the remainder* 1 *on dividing by* 9.

□ On the one hand, for the number 28, it is obvious.

On the other hand, for any even perfect number $2^{p-1}(2^p - 1)$, greater than 28, the number p is a prime greater 3, i.e., $p \equiv \pm 1 (mod\ 6)$. If $p = 6l + 1$, then

$$2^{p-1}(2^p - 1) \equiv (2^6)^l (2(2^6)^l - 1) \equiv 1 (mod\ 9).$$

If $p = 6l + 5$, then

$$2^{p-1}(2^p - 1) \equiv 2^4(2^6)^l(2^5(2^6)^l - 1) \equiv 16(32 - 1) \equiv 7 \cdot 4 \equiv 1 (mod\ 9). \ \square$$

In fact, the proof of the fact that any even perfect number greater than 6 gives the remainder 1 on dividing by 9 can be obtained using the following property: *Any even perfect number greater than 6 has the form* $1 + 9S_3(n)$. We consider this property in the next section.

Now, we can check that

- *adding the decimal digits of any even perfect number greater than* 6*, then adding the digits of the resulting number, and repeating this process until a single digit is obtained always produces the number* 1.

□ The proof is based on the fact that for a given positive integer

$$n = (c_s c_{s-1} \dots c_1 c_0)_g = c_s g^s + c_{s-1} g^{s-1} + \cdots + c_1 g + c_0,$$
$$0 \leq c_i \leq 9, c_s \neq 0,$$

in base 10, the sum $c_s + \cdots + c_1 + c_0$ of the decimal digits of n is congruent to n modulo 9.

As any even perfect number greater than 6 is congruent to 1 modulo 9, we get a decreasing sequence of positive integers, each term of which is congruent to 1 modulo 9. Obviously, this sequence ends by 1 after finite number of steps. □

For example, for the number 28, we have $2+8=10$ and $1+0=1$; for the number 496, we have $4+9+6=19$, $1+9=10$, $1+0=1$; for 8128, we have $8+1+2+8=19$, $1+9=10$, and $1+0=1$.

Recall that the *digital root* (or *repeated digital sum*) of a positive integer n is defined as the (single-digit) value obtained by an iterative process of summing digits on each iteration using the result from the previous iteration to compute a digital sum if the process continues until a single-digit number is reached.

Therefore, the property above can be reformulated as follows:

- *The digital root of every even perfect number other than* 6 *is* 1.

Note that this property holds for all positive integer numbers of the form $2^{k-1}(2^k - 1)$ for any odd integer k.

3.3.7. In terms of representation of an even perfect number in base 9, we can reformulate the previous property as follows:

- *The last digit of the representation of any even perfect number greater* 6 *in base* 9 *is* 1.

As for base 2, each even perfect number has very precise form. For example, for the first four even perfect numbers, we have:

$$6_{10} = 2^2 + 2^1 = 110_2;$$
$$28_{10} = 2^4 + 2^3 + 2^2 = 11100_2;$$
$$496_{10} = 2^8 + 2^7 + 2^6 + 2^5 + 2^4 = 111110000_2;$$
$$8128_{10} = 2^{12} + 2^{11} + 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 = 1111111000000_2.$$

In fact, it is easy to prove that

- *every even perfect number* $2^{p-1}(2^p - 1)$ *is represented in binary form as p ones followed by* $p - 1$ *zeros.*

□ We can check this using simple arithmetic in base 2: $2^{p-1} = 100...0_2$, where the representation has exactly $p - 1$ zeros, and $2^p - 1 = 100...0_2 - 1 = 111...1_2$, where the representation has exactly p ones; so,

$$2^{p-1}(2^p - 1) = 100\ldots0_2 \cdot 111\ldots1_2 = 11\ldots100\ldots0_2,$$

with p ones and $p - 1$ zeros. □

It means that every even perfect number is a *pernicious number*, i.e., a positive integer such that the number of ones in its binary representation (in fact, its *Hamming weight*) is a prime.

We consider this connection of perfect numbers later in Section 3.5.

For the representation of even perfect numbers in base 4, we can obtain similar results. For example, for the first four even perfect numbers, we have:

$6_{10} = 4^1 + 2 = 12_4$;
$28_{10} = 4^2 + 3 \cdot 4^1 = 130_4$;
$496_{10} = 4^4 + 3 \cdot 4^3 + 3 \cdot 4^2 = 13300_4$;
$8128_{10} = 4^6 + 3 \cdot 4^5 + 3 \cdot 4^4 + 3 \cdot 4^3 = 1333000_4$.

It is easy to show that

- *every even perfect number* $2^{p-1}(2^p-1)$ *greater than* 6 *is represented in base* 4 *as one unity followed by* $\frac{p-1}{2}$ *threes and then followed by* $\frac{p-1}{2}$ *zeros.*

□ We can check this using simple arithmetic in base 4. As for odd p, it holds that

$$2^{p-1}(2^p - 1) = 4^{\frac{p-1}{2}}(2 \cdot 4^{\frac{p-1}{2}} - 1),$$

$4^{\frac{p-1}{2}} = 100\ldots0_4$, where the representation has exactly $\frac{p-1}{2}$ zeros, $2 \cdot 4^{\frac{p-1}{2}} = 200\ldots0_4$, where the representation has exactly $\frac{p-1}{2}$ zeros, and hence, $2 \cdot 4^{\frac{p-1}{2}} - 1 = 233\ldots3_4$, where the representation has exactly $\frac{p-1}{2}$ threes, we get

$$\begin{aligned}2^{p-1}(2^p-1) &= 4^{\frac{p-1}{2}}(2\cdot 4^{\frac{p-1}{2}}-1) = 100\ldots 0_4(200\ldots 00_4-1)\\ &= 100\ldots 00_4 \cdot 133\ldots 33_4 = 133\ldots 300\ldots 0_4,\end{aligned}$$

where the representation has exactly $\frac{p-1}{2}$ threes and exactly $\frac{p-1}{2}$ zeros. □

Different representations of perfect numbers

3.3.8. As was considered above, any even perfect number is defined by a Mersenne prime: If $M_p = 2^p - 1$ is prime, then $2^{p-1}(2^p-1)$ is perfect. So, we can note that

- *if M_p is a Mersenne prime, then $\frac{M_p(M_p+1)}{2}$ is an even perfect number.*

□ The proof is obvious. As $M_p = 2^p - 1$, $M_p + 1 = 2^p$, and $\frac{M_p+1}{2} = 2^{p-1}$, we get that $\frac{M_p(M_p+1)}{2} = 2^{p-1}(2^p-1)$, where $2^p-1 \in P$. □

3.3.9. So, we can represent any even perfect number as $\frac{N(N+1)}{2}$. Now, it is easy to check that *any even perfect number is a triangle number*. More precisely,

- *if $2^p-1 \in P$, then $2^{p-1}(2^p-1) = S_3(2^p-1)$.*

□ It follows from the definition of the nth triangle number that

$$S_3(n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Since $2^{p-1}(2^p-1) = \frac{(2^p-1)2^p}{2}$, we get that $\frac{2^{p-1}(2^p-1)}{2} = S_3(2^p-1)$. □

So, we can state that

- *any even perfect number $2^{p-1}(2^p-1)$ is the triangle number with the prime index 2^p-1, coinciding with the odd part of a given perfect number.*

Moreover,

- *the* n*th even perfect number* $2^{p-1}(2^p-1)$ *is the triangle number with the index* 2^p-1 *equal to the* n*th Mersenne prime.*

In fact, the first (even) perfect number 6 is the third triangle number, where $3 = 2^2 - 1$ is the first Mersenne prime. The second (even) perfect number 28 is the seventh triangle number, where $7 = 2^3 - 1$ is the second Mersenne prime. The third (even) perfect number 496 is the 31st triangle number, where $31 = 2^5 - 1$ is the third Mersenne prime. The fourth (even) perfect number 8128 is the 127th triangle number, where $31 = 2^5 - 1$ is the fourth Mersenne prime, etc. The 48th (even) perfect number $2^{57885160}(2^{57885161} - 1) = 169296\ldots 130176$ (34850340 digits) is the $(2^{57885161} - 1)$th triangle number, where $2^{57885161} - 1 = 581887\ldots 285951$ (17425170 digits) is the 48th Mersenne prime. It was found in 2013. There are three more known Mersenne primes M_p with $p \in \{74207281, 77232917, 82589933\}$, but it has not been verified whether any undiscovered Mersenne primes exist between the 48th Mersenne prime, $M_{57885161}$, and the biggest known Mersenne prime, $M_{82589933}$.

Moreover, it is possible to show that

- *any even perfect number greater than* 6 *is the triangle number* $S_3(3n+1)$, *where the index* $3n+1$ *is a prime number and* $n \equiv 2(mod\ 8)$.

□ In fact, if the even perfect number $2^{p-1}(2^p-1)$ is greater than 6, then as $2^p - 1$ is prime, it holds that p is an odd number greater than 1. In this case,

$$2^p - 1 = 2^{2l+1} - 1 = 2 \cdot 4^l - 1 \equiv 2 - 1 \equiv 1(mod\ 3),$$

i.e., $2^p - 1 = 3n + 1$.

Moreover, for $p \geq 3$, it holds that $2^p - 1 \equiv -1(mod\ 8)$, i.e., $3n + 1 \equiv -1(mod\ 8)$, $3n \equiv -2 \equiv 6(mod\ 8)$, and as $gcd(3, 8) = 1$, (the numbers 3 and 8 are relatively prime, and one can divide the last congruence by 3), $n \equiv 2(mod\ 8)$. □

For example, $28 = S_3(7) = S_3(3 \cdot 2 + 1)$, and $2 \equiv 2(mod\ 8)$; $496 = S_3(31) = S_3(3 \cdot 10 + 1)$, $10 \equiv 2(mod\ 8)$; $8128 = S_3(127) = S_3(3 \cdot 42 + 1)$, and $42 \equiv 2(mod\ 8)$.

Using the last result, we can prove that

- *any even perfect number greater than* 6 *has the form* $1 + 9S_3(n)$, *where* $n \equiv 2(mod\ 8)$.

□ Really, any even perfect number greater than 6 is a triangle number with the prime index of the form $3n+1$, where $n \equiv 2(mod\ 8)$. In turn,

$$S_3(3n+1) = \frac{(3n+1)(3n+2)}{2} = \frac{9n(n+1)+2}{2}$$
$$= 1 + 9 \cdot \frac{n(n+1)}{2} = 1 + 9S_3(n).$$

The property is proven. □

It is easy to show that in this case, $S_3(n) = S_3(\frac{2^p-2}{3}) \equiv 3, 5(mod\ 10)$.

So, starting with the perfect numbers $S_3(7) = 28$, $S_3(31) = 496$, $S_3(127) = 8128$, etc., we get after subtracting 1 from the perfect number and dividing the result by 9 the new triangle numbers $S_3(2) = 3$, $S_3(10) = 55$, $S_3(42) = 903$, $S_3(2730) = 3727815$, etc. ending in 3 or 5.

So, we got the connection between even perfect numbers and triangular numbers. In fact, any even perfect number is triangular.

If we consider only the odd part of a given perfect number, i.e., a given Mersenne prime $M_p = 2p - 1$, we can prove that

- *the only one Mersenne prime is triangular: It is* $M_2 = S_3(2)$.

More generally, it holds that $M_1 = S_3(1)$, $M_2 = S_3(2)$, $M_4 = S_3(4)$, and $M_{12} = S_3(90)$, and it is possible to prove that $M_n = 2^n - 1$, $n \in \mathbb{N}$ *is a triangle number only for these four cases.*

The problem of finding all triangular Mersenne numbers is equivalent to the problem of finding all positive integer solutions of the *Ramanujan–Nagell equation* $2^n - 7 = x^2$. The solutions of this equation in positive integers n and x exist just when $n = 3$, 4, 5, 7, and 15 (sequence A060728 in the OEIS) with corresponding $x = 1$, 3, 5, 11, and 181 (sequence A038198 in the OEIS), as was conjectured by the Indian mathematician S. Ramanujan and proved by the Norwegian mathematician T. Nagell.

In this case, if the number $M_v = 2^v - 1$ is triangular, then the values of v are just those of $n - 3$ so that the triangular Mersenne numbers are 1, 3, 15, 4095 (see sequence A076046 in the OEIS) and no more.

The numbers 0, 1, 3, 15, and 4095, which are the only non-negative integers which have simultaneously the form $\frac{u(u+1)}{2}$, $u = 0, 1, 2, \ldots$ and the form $2^v - 1$, $v = 0, 1, 2, \ldots$ are also called *Ramanujan–Nagell numbers.*

3.3.10. Moreover, it is easy to show that

- *any even perfect number is an hexagonal number.*

□ Recall that the nth hexagonal number $S_6(n)$ is defined as the number of distinct dots in a pattern of dots consisting of the outlines of regular hexagons with sides up to n dots when the hexagons are overlaid so that they share one vertex. In other words,

$$S_6(n) = 1 + 5 + 9 + \cdots + (4n - 3) = n(2n - 1).$$

For $n = 2^{p-1}$, we get

$$S_6(n) = S_6(2^{p-1}) = 2^{p-1}(2 \cdot 2^{p-1} - 1) = 2^{p-1}(2^p - 1).$$

So, if $2^p - 1$ is a prime, the (2^{p-1})th hexagonal number $S_6(2^{p-1})$ coincides with the perfect number $2^{p-1}(2^p - 1)$.

The same result can be obtained as follows. As $n(2n - 1) = \frac{2n(2n-1)}{2}$, it holds that $S_6(n) = S_3(2n - 1)$. So, since for a prime number $2^p - 1$, the $(2^p - 1)$th triangular number $S_3(2^p - 1)$ gives an even perfect number $2^{p-1}(2^p - 1)$, we can get the same perfect number as the hexagonal number with the index $\frac{(2^p-1)+1}{2} = 2^{p-1}$. □

So, we have proven that

- *for the number* $2^{p-1}(2^p - 1)$, $2^p - 1 \in P$, *it holds that* $2^{p-1}(2^p - 1) = S_6(2^{p-1})$.

In other words, we can state that

- *the even perfect number* $2^{p-1}(2^p - 1)$ *is the hexagonal number with the index equal to a power of two of the form* 2^{p-1}*, where* $p \in P$ *and coinciding with the even part of a given perfect number.*

In fact, the first (even) perfect number 6 is the second hexagonal number, where $2 = 2^{2-1}$, and $2^2 - 1 = 3$ is the first Mersenne prime. The second (even) perfect number 28 is the fourth hexagonal number, where $4 = 2^{3-1}$, and $2^3 - 1 = 7$ is the second Mersenne prime. The third (even) perfect number 496 is the 16th hexagonal number, where $16 = 2^{5-1}$, and $2^5 - 1 = 31$ is the third Mersenne prime. The fourth (even) perfect number 8128 is the 64th hexagonal number, where $64 = 2^{7-1}$, and $2^7 - 1 = 127$ is the fourth Mersenne prime, etc. The 48th (even) perfect number $2^{57885160}(2^{57885161} - 1) = 169296\ldots130176$ (34850340 digits) is $(2^{57885160})$th hexagonal number, where $2^{57885160} = 2^{57885161-1}$, and $2^{57885161} - 1$ (17425170 digits) is the 48th Mersenne prime. It was found in 2013. There are three more known Mersenne primes M_p with $p \in \{74207281, 77232917, 82589933\}$, and hence three more even perfect numbers (not necessarily 49th, 50th, and 51st even perfect numbers, as it has not been verified whether any undiscovered Mersenne primes exist between the 48th Mersenne prime $M_{57885161}$ and the biggest known Mersenne prime $M_{82589933}$), which can be represented as $2^{74207280}$th, $2^{77232916}$th, and $2^{82589932}$th hexagonal numbers, correspondingly.

3.3.11. So, we have proven that any even perfect number is a triangular and a hexagonal number. On the other hand, *any even perfect number cannot be a square number*:

- *For* $2^{p-1}(2^p - 1)$, $2^p - 1 \in P$*, it holds that* $2^{p-1}(2^p - 1) \neq a^2$ $a \in \mathbb{Z}$.

□ This is obvious because the prime number $2^p - 1$ is represented in the number $2^{p-1}(2^p - 1)$ only one time. □

The reader can see that most properties listed in this section are proven only for even perfect numbers. However, it is easy to prove that

- *any perfect number, even or odd, cannot be a perfect square.*

□ As we have proven already this fact for any even perfect number, let us consider now an odd perfect number n. If it is a perfect square, its prime decomposition should have the form $n = p_1^{2\alpha_1} p_2^{2\alpha_2} \dots p_k^{2\alpha_k}$, where $p_1 < p_2 < \cdots < p_k$ are some odd prime numbers, and $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}$. It is easy to see that for any odd prime p, the value $\sigma(p^{2\alpha}) = 1 + p + \cdots + p^{2\alpha}$ can be represented as a sum of odd number of odd numbers and therefore is an odd positive integer. As the sigma function is multiplicative, it holds that $\sigma(n) = \sigma(p_1^{2\alpha_1} p_2^{2\alpha_2} \dots p_k^{2\alpha_k}) = \sigma(p_1^{2\alpha_1})\sigma(p_2^{2\alpha_2}) \dots \sigma(p_k^{2\alpha_k})$ is also an odd positive integer. But for a perfect number n, it holds that $\sigma(n) = 2n$, so $\sigma(n)$ should be even; a contradiction. □

Now, it is east to show that, for example,

- *any perfect number, even or odd, cannot to be a biquadratic number.*

Moreover, *any perfect number, even or odd, cannot to be any nontrivial even power*:

- *For any* $p \in P$ *such that* $2^p - 1 \in P$, *it holds that* $2^{p-1}(2^p - 1) \neq k^{2s}$, *where* $k, s \in \mathbb{N}$.

□ This fact is trivial: If $2^{p-1}(2^p - 1) = k^{2s}$, we get a representation of an even perfect number as a perfect square $(k^s)^2$. The same arguments hold for any odd perfect number. □

3.3.12. Furthermore, we can show that

- *each even perfect number greater than* 6 *is a centered nonagonal number.*

□ Recall that a *centered nonagonal number* (or *centered enneagonal number*) is a positive integer number that represents a nonagon with a dot in the center and all other dots surrounding the central dot in successive nonagonal layers. The nth centered nonagonal number is given by the formula

$$\overline{S}_9(n) = 1 + 9 + 18 + \cdots + 9(n-1) = \frac{(3n-2)(3n-1)}{2}.$$

So, for $n = \frac{2^p+1}{3}$, where $p \in P\backslash\{2\}$, we get

$$\overline{S}_9(n) = \frac{(3n-2)(3n-1)}{2} = \frac{(2^p-1)2^p}{2} = 2^{p-1}(2^p-1).$$

It means that in the case of primality of the number $2^p - 1$ with odd prime p, the $(\frac{2^p+1}{3})$th-centered nonagonal number coincides with the even perfect number $2^{p-1}(2^p-1)$.

However, the same result can be obtained as follows. It is obvious that

$$\overline{S}_9(n) = \frac{(3n-2)(3n-1)}{2} = S_3(3n-2),$$

i.e., any centered nonagonal number is a triangular number. But any even perfect number is also a triangular number: $2^{p-1}(2^p-1) = S_3(2^p-1)$. So, representing $2^p - 1$ as $3n - 2$, we get for n the integer value $\frac{2^p+1}{3}$; in this case, $2^{p-1}(2^p-1) = \overline{S}_9(n)$.

3.3.13. In the end of our consideration, note that

- *even perfect numbers cannot be represented as the difference of two positive non-consecutive triangular numbers.*

That means that there is no even perfect number which is a *trapezoidal number.*

□ In fact, there are exactly three types of non-trapezoidal numbers: even perfect numbers, powers of two, and the numbers of the form $2^{n-1}(2^n+1)$ formed as the product of a Fermat prime $2^n + 1$ with a power of two in a similar way to the construction of even perfect numbers from Mersenne primes. □

We consider this question in Section 3.5.

Sum-representations of perfect numbers

3.3.14. As a triangle number, *any even perfect number is a sum of consecutive positive integers starting from 1 up to a Mersenne prime.* In fact,

- *for* $2^p - 1 \in P$, *it holds that* $2^{p-1}(2^p - 1) = 1 + 2 + \cdots + (2^p - 2) + (2^p - 1)$.

□ It follows from the equality $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ used for $n = 2^p - 1$:

$$2^{p-1}(2^p-1) = S_3(2^p-1) = \frac{(2^p - 1)2^p}{2} = 1+2+\cdots+(2^p-2)+(2^p-1).$$

If the condition $2^p - 1 \in P$ holds, we get the needed representation of a given even perfect number $2^{p-1}(2^p - 1)$. □

Moreover, for the nth even perfect number, the corresponding sum of consecutive positive integers starting from 1 is terminating on the nth Mersenne prime.

In fact, the first (even) perfect number 6 is represented as $6 = 1 + 2 + 3$, where $3 = 2^2 - 1$ is the first Mersenne prime. The second (even) perfect number 28 is represented as $28 = 1+2+3+4+5+6+7$, where $7 = 2^3 - 1$ is the second Mersenne prime. The third (even) perfect number 496 is represented as $496 = 1 + 2 + \cdots + 30 + 31$, where $31 = 2^5 - 1$ is the third Mersenne prime. The fourth (even) perfect number 8128 is represented as $8128 = 1 + 2 + \cdots + 126 + 127$, where $127 = 2^7 - 1$ is the fourth Mersenne prime, etc. The 48th (even) perfect number $2^{57885160}(2^{57885161} - 1) = 169296\ldots130176$ (34850340 digits) is represented as $169296\ldots130176 = 1 + 2 + \cdots + (2^{57885161} - 2) + (2^{57885161} - 1)$, where $2^{57885161} - 1 = 581887\ldots285951$ (17425170 digits) is the 48th Mersenne prime. It was found in 2013. There are three more known Mersenne primes M_p with $p \in \{74207281, 77232917, 82589933\}$ and hence three more even perfect numbers (not necessary 49th, 50th, and 51st even perfect numbers), which can be represented as $1+2+\cdots+(2^{74207281}-2)+(2^{74207281}-1)$, $1+2+\cdots+(2^{77232917}-2)+(2^{77232917}-1)$, and $1+2+\cdots+(2^{82589933} - 2) + (2^{82589933} - 1)$, correspondingly.

Moreover, it is possible to show that

- *any even perfect number* $2^{p-1}(2^p-1)$*, greater than* 6*, is a sum of the first* $2^{\frac{p-1}{2}}$ *odd cubes*:

$$2^{p-1}(2^p-1)=\sum_{i=1}^{2^{\frac{(p-1)}{2}}}(2i-1)^3.$$

□ For the proof, consider an odd number q. As $1^3+\cdots+q^3=\frac{q^2(q+1)^2}{4}$ and $1^3+\cdots+(\frac{q-1}{2})^3=\frac{(\frac{q-1}{2})^2(\frac{q-1}{2}+1)^2}{4}$ ([Step01]), then $2^3+4^3+\cdots+(q-1)^3=2(\frac{q-1}{2})^2(\frac{q-1}{2}+1)^2$, and

$$\begin{aligned}1^3+3^3+\cdots+q^3&=\frac{q^2(q+1)^2}{4}-2\left(\frac{q-1}{2}\right)^2\left(\frac{q-1}{2}+1\right)^2\\&=\frac{2q^2(q+1)^2-(q-1)^2(q+1)^2}{8}\\&=\frac{(q+1)^2(q^2+2q-1)}{8}\\&=\frac{(\frac{q^2+2q-1}{2})(\frac{q^2+2q-1}{2}+1)}{2},\end{aligned}$$

i.e., it holds that

$$1^3+3^3+\cdots+q^3=S_3\left(\frac{q^2+2q-1}{2}\right).$$

We get now our result for $q=2^{\frac{p+1}{2}}-1$. In this case,

$$\frac{q^2+2q-1}{2}=\frac{1}{2}((2^{\frac{p+1}{2}}-1)^2+2(2^{\frac{p+1}{2}}-1)-1)=\frac{1}{2}(2^{p+1}-2)=2^p-1,$$

and $S_3(2^p-1)=2^{p-1}(2^p-1)$. □

For example, $28=2^2(2^3-1)$; in this case, $p=3$ and $2^{\frac{p+1}{2}}-1=3$; so, $28=1^3+2^3$. $496=2^4(2^5-1)$; in this case $p=5$ and $2^{\frac{p+1}{2}}-1=7$; so, $496=1^3+3^3+5^3+7^3$. $8128=2^6(2^7-1)$; in this case $p=7$ and $2^{\frac{p+1}{2}}-1=15$; so, $8128=1^3+3^3+\cdots+15^3$.

3.3.15. As a hexagonal number, *an even perfect number can be represented as a sum of the first* 2^{p-1} *elements of arithmetic progression* $1, 5, 9, \ldots$. In fact,

- *for* $2^p - 1 \in P$, *it holds that* $2^{p-1}(2^p - 1) = \sum_{k=0}^{n-1}(4k+1)$ *with* $n = 2^{p-1}$.

□ In follows from the definition of a hexagonal number that $S_6(n) = 1 + 5 + 9 + \cdots + (4n - 3)$. As $2^{p-1}(2^p - 1) = S_6(2^{p-1})$, we get the decomposition

$$2^{p-1}(2^p - 1) = 1+5+9+\cdots+(4\cdot 2^{p-1} - 3) = 1+9+\cdots+(2^{p+1} - 3).$$

□

For example, $6 = 2^1(2^2 - 1)$; in this case, $p = 2$ and $2^{p-1} = 2$, while $2^{p+1} - 3 = 5$; so, $6 = 1 + 5$; $28 = 2^2(2^3 - 1)$; in this case, $p = 3$ and $2^{p-1} = 4$, while $2^{p+1} - 3 = 13$; so, $28 = 1 + 5 + 9 + 13$. $496 = 2^4(2^5 - 1)$; in this case, $p = 5$ and $2^{p-1} = 16$, while $2^{p+1} - 3 = 61$; so, $496 = 1+5+9+13+17+21+25+29+33+37+41+45+49+53+57+61$; $8128 = 2^6(2^7 - 1)$; in this case, $p = 7$ and $2^{p-1} = 64$, while $2^{p+1} - 3 = 253$; so, $8128 = 1 + 5 + 9 + 13 + 17 + 21 + 25 + 29 + 33 + 37 + 41 + 45 + 49 + \cdots + 245 + 249 + 253$.

Properties of divisors of perfect numbers

3.3.16. Divisors of perfect numbers play a very important role in the theory of these numbers. In fact, the definition of a perfect number is based on the notion of positive integer divisor: a positive integer n is perfect if the sum of its proper divisors is n. In other words, $s(n) = n$, where $s(n) = \sum_{d|n,\ d\neq n} d$ is the *aliquot sum function* (or *restricted divisor function*). In this case, the sum of all positive integer divisors of n is $2n$, i.e., $\sigma(n) = 2n$, where $\sigma(n) = \sum_{d|n} d$ is the *sum of divisors function* (or *sigma function*).

So, it is obvious that

- *for any perfect number, even or odd, the sum of all its positive integer divisors is even.*

□ Of course, as $\sigma(n) = 2n$, then $\sigma(n)$ is even. □

For even perfect numbers, having a very precise form due to the Euclid–Euler theorem, this result can be reformulated in terms of Mersenne primes:

- *For* $M_p = 2^p - 1 \in P$, *it holds that* $\sigma(\frac{M_p(M_p+1)}{2}) = M_p(M_p + 1)$.

It is easy to show that, moreover,

- *for any perfect number, even or odd, the number of all its positive integer divisors is even.*

□ It was proven before that any perfect number, even or odd, cannot be a perfect square. It means that his prime decomposition $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, $p_1 < \cdots < p_k \in P$, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$, contains a term of the form $p^{2\beta+1}$, i.e., a prime number p, which is represented in this decomposition with an odd degree $2\beta + 1$. In this case,

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1) = (\beta + 2)K, \ K \in \mathbb{N},$$

i.e., $\tau(n)$ is even. □

For even perfect numbers, we can obtain some additional information. In fact,

- *for any even perfect number, the number of all its positive integer divisors is twice of a prime.*

□ Really, any even perfect number has the form $2^{p-1}(2^p - 1)$, where the number $2^p - 1$ is prime, and we have $\tau(2^{p-1}(2^p - 1)) = 2p$. □

So, we can state that

- *for the nth even perfect number, the value of the tau function is* $2p$*, where prime* p *is the index of the nth Mersenne prime.*

In fact, the first (even) perfect number $6 = 2 \cdot 3$ has four divisors, i.e., $\tau(6) = 2 \cdot 2$, where 2 is the index of $M_2 = 3 = 2^2 - 1$, the first Mersenne prime. The second (even) perfect number $28 = 2^2 \cdot 7$ has 6 divisors, i.e., $\tau(28) = 2 \cdot 3$, where 3 is the index of $M_3 = 7 = 2^3 - 1$, the second Mersenne prime. The third (even) perfect number $496 = 2^4 \cdot 31$ has 10 divisors, i.e., $\tau(496) = 2 \cdot 5$, where 5 is the index of $31 = 2^5 - 1$, the third Mersenne prime. The fourth (even) perfect number 8128 $8128 = 2^6 \cdot 127$ has 14 divisors, i.e., $\tau(8128) = 2 \cdot 7$, where 7 is the index of $M_7 = 127 = 2^7 - 1$, the fourth Mersenne prime, etc. The 48th (even) perfect number $2^{57885160}(2^{57885161} - 1) = 169296\ldots130176$ (34850340 digits) has $2 \cdot 57885161 = 114770322$ divisors, where 57885161 is the index of $M_{57885161} = (2^{57885161} - 1) = 581887\ldots285951$ (17425170 digits), the 48th Mersenne prime.

One more elementary but important fact about divisors of any even perfect number can be formulated as follows:

- *For any even perfect number, it holds that the odd part of its prime factorization is equal to the sum of the divisors of the even part of this factorization, while the even part of its prime factorization is equal to the one half of the sum of the divisors of the odd part of this factorization.*

☐ This follows from Leonhard Euler's result that an even perfect number must have the form $2^{p-1}(2^p-1)$, $2^p-1 \in P$. The odd part of this factorization is 2^p-1; it is equal to $1+2+2^2+\cdots+2^{p-1}$, the sum of the divisors of the even part 2^{p-1} of this factorization. On the other hand, the sum of the divisors of the odd part 2^p-1 is $1+(2^p-1)$; it is equal to 2^p, twice the even part 2^{p-1} of our factorization. ☐

3.3.17. As for the aliquot sum function $s(n)$, we can state that

- *for an even perfect number n, the value $s(n)$ of the aliquot sum function is even, while for an odd perfect number n, the value $s(n)$ of the aliquot sum function is odd.*

☐ This follows from the fact that $s(n)=\sigma(n)-n$; so, for any perfect number n, it holds that $s(n)=n$, and the proposition becomes obvious. ☐

Much more important is the following property:

- *Any perfect number is a fixed point of the restricted divisor function $s(n)=\sigma(n)-n$, and the aliquot sequence associated with a perfect number is a constant sequence.*

☐ In fact, an *aliquot sequence* is the sequence of numbers obtained by repeatedly applying the restricted divisor function $s(n)=\sigma(n)-n$ to n.

If the period of the aliquot cycle is 1, i.e., $s(n)=n$, we get a perfect number. For example, the aliquot sequence for 6 is 6,6,6,... .

If the period is 2, i.e., $s(n)=m$, and $s(m)=n$, the two obtained numbers n, m form an amicable pair.

If the period is $t \geq 3$, we get a group of sociable numbers. □

We consider these questions in Chapters 4 and 5.

3.3.18. It is easy to see that

- *the sum of the reciprocities to all positive integers divisors of a given perfect number n is equal to* 2.

□ In fact, a positive divisor d of a positive integer n corresponds to the positive integer divisor $\frac{n}{d}$ of the same number n. They coincide only if $n = t^2$; in this case, $d = \frac{n}{d} = t$. Using the definition $\sigma(n) = 2n$ and the consideration above, we get the equality

$$\sigma(n) = d_1 + \cdots + d_s = \frac{n}{d_1} + \cdots + \frac{n}{d_s} = 2n,$$

and hence the equality

$$\frac{1}{d_1} + \cdots + \frac{1}{d_s} = 2.$$

For example, for the number 6, we have $\frac{1}{6} + \frac{1}{3} + \frac{1}{2} + \frac{1}{1} = 2$; for the number 28, we have $\frac{1}{28} + \frac{1}{14} + \frac{1}{7} + \frac{1}{4} + \frac{1}{2} + \frac{1}{1} = 2$, etc. □

A positive integer is called *Ore harmonic number* if the harmonic mean of its divisors is an integer. So, as the number of divisors of any perfect number is even, we get that

- *any perfect number is an Ore harmonic number.*

3.3.19. There exists also the following "criteria of perfectness":

- *A positive integer n is a perfect number if and only if*

$$1\cdot\left\lfloor\frac{n}{1}\right\rfloor+\cdots+(n-2)\left\lfloor\frac{n}{n-2}\right\rfloor = 1+1\cdot\left\lfloor\frac{n-1}{1}\right\rfloor+\cdots+(n-1)\left\lfloor\frac{n-1}{n-1}\right\rfloor.$$

□ In fact, using the property

$$\sum_{i=1}^{n} \sigma(i) = \sum_{i=1}^{n} i\left\lfloor\frac{n}{i}\right\rfloor$$

and the obvious equalities $\left\lfloor \frac{n}{n} \right\rfloor = 1$, $n \geq 1$, $\left\lfloor \frac{n}{n-1} \right\rfloor = 1$, $n \geq 3$, we get that

$$\sum_{i=1}^{n-2} i \left\lfloor \frac{n}{i} \right\rfloor = 1 + \sum_{i=1}^{n-1} i \left\lfloor \frac{n-1}{i} \right\rfloor,$$

if and only if

$$\sum_{i=1}^{n} \sigma(i) - (n-1) \left\lfloor \frac{n}{n-1} \right\rfloor - n \left\lfloor \frac{n}{n} \right\rfloor = 1 + \sum_{i=1}^{n-1} \sigma(i),$$

i.e., if and only if $\sigma(n) = 2n$. □

Other properties of perfect numbers

3.3.20. One can prove (Makowski, 1962) that

- *the only even perfect number of the form* $x^3 + 1$ *is* 28.

Moreover, it is proven (Gallardo, 2010) that the sum $28 = 3^3 + 1^3$ is the only possible representation of an even perfect number as a sum of two perfect cubes:

- 28 *is the only even perfect number that is a sum of two positive cubes of integers.*

3.3.21. The distribution of perfect numbers can be characterized by the function $A(x)$, which counts the number of perfect numbers less than or equal to a positive real number x. For example, $A(1) = 0$, $A(10) = 1$, $A(30) = 2$, etc. It is proven (see Kanold, 1956) that

- *for the number* $A(x)$ *of perfect numbers less than or equal to* x*, it holds that*

  $$A(x) \leq c\sqrt{x},$$

  where $c > 0$ *is an absolute constant.*

In other words, $A(x) = O(\sqrt{x})$.

For some additional information, see, for example, in [Buch09], [Kano56] [Deza17], [Deza18], [Sier64], [Dick05], [Step01], [Wiki22], and [Yan96].

Exercises

1. Using the fact that even perfect numbers are of the form $S_3(2^p-1)$, where $S_3(n)$ is the nth triangle number, find resulting triangular numbers for the first 10 even perfect numbers.
2. Check that even perfect numbers greater 6 are of the form $1+9\cdot S_3(\frac{2^p-2}{3})$, where $S_3(n)$ is the nth triangle number; find the first 10 resulting triangular numbers. Prove that their last decimal digit is 3 or 5.
3. Prove that every even perfect number ends in 6 or 28, base 10.
4. Prove that every even perfect number greater than 6 ends in 1, base 9. Find such representations for the first four even perfect numbers.
5. Prove that adding the digits of any even perfect number greater than 6, then adding the digits of the resulting number, and repeating this process until a single digit (called the digital root) is obtained always produces the number 1. Check this for the first four even perfect numbers greater than 6.
6. Prove that the digital root of any number $2^{k-1}(2^k-1)$ with odd k is equal to 1. Check it for all odd $k \leq 10$. What can be said about the digital root of numbers $2^{k-1}(2^k+1)$ with odd k? What can be said about the digital root of numbers $2^{k-1}(2^k+1)$ with prime 2^k+1?
7. Prove that the only square-free (even) perfect number is 6. Find the square part of an even perfect number. Find a square-free part of an even perfect number. Which connections exist between these two positive integer numbers?

3.4. Search for Perfect Numbers

3.4.1. In the theory of perfect, amicable, and sociable numbers, there exist three classical groups of methods for finding all these three kinds of special numbers. There are three essentially different types of methods of such generation, namely the exhaustive numerical searching methods, the algebraic assumption methods, and the algebraic constructive methods (for more information, see, for example, the monograph of S. Y. Yan [Yan96].

Methods of the first type are directly based on numerical calculations of values of the sigma function. For example, if $\sigma(N) = 2N$, then N is a perfect number. On the other hand, if $\sigma(N) = \sigma(M) = N + M$, then the numbers M and N form an amicable pair (M, N).

In the second type of methods, an assumption is made about the prime structure of considered numbers. For example, for $k = 1, 2, 3, \ldots$, if $2^k - 1$ is a prime, then $N = 2^{k-1}(2^k - 1)$ is an even perfect number. On the other hand, for $n = 1, 2, 3, \ldots$, if p, q, and r are distinct primes of a special form, then the numbers $M = 2^n pq$ and $N = 2^n r$ form an amicable pair (M, N).

In the third type of methods, new elements of considered set of special numbers are constructed from a given (*breeder*) element of the same set. We consider such algorithms for constructing large amicable pairs in Chapter 4.

In this section, we present main facts concerning the historical and contemporary aspects of the search for perfect numbers.

For this class of special numbers, two types of searching methods are used: exhaustive numerical methods (based on the fact that $\sigma(N) = 2N$ for a perfect number) and algebraic assumption methods (based on the Euclid–Euler theorem, i.e., connected with the search for new large Mersenne primes).

Numerical methods for perfect numbers

3.4.2. The numerical methods are the simplest methods, in which the computation is directly based on the calculation of the sigma function.

Recall that a positive integer is deficient, perfect, or abundant if $\sigma(n) < 2n$, $\sigma(n) = 2n$, or $\sigma(n) > 2n$, respectively. So, the determination of where n is deficient, perfect, or abundant can be done by just checking the sigma value of n. Therefore, we get the following simplest numerical method.

Algorithm for searching all deficient, perfect, and abundant numbers in the interval $[\boldsymbol{A}, \boldsymbol{B}]$.

- For n from A to B, find

$$\sigma(n) = \sigma(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+1} - 1}{p_s - 1};$$

- if $\sigma(n) < 2n$, then n is deficient;
- if $\sigma(n) = 2n$, then n is perfect;
- if $\sigma(n) > 2n$, then n is abundant.

Note that most computer algebra systems (Mathematica, Marple, etc.) have a standard function to calculate $\sigma(n)$.

For $n \in [1, 30]$, we have the following result. Similar algorithms can be used for searching other classes of special numbers, which are

Deficient	Perfect	Abundant
1	6	12
2	28	18
3		20
4		24
5		30
7		
8		
9		
10		
11		
15		
16		
17		
19		
21		
22		
23		
25		
26		
27		
29		

defined in terms of the sigma function: k-perfect numbers, $k = 3, 4, 5, \ldots$, with $\sigma(n) = kn$; almost perfect numbers with $\sigma(n) = 2n-1$; quasiperfect numbers with $\sigma(n) = 2n+1$; superperfect numbers with $\sigma(\sigma(n)) = 2n$, etc. We consider these classes of special numbers in Chapter 5.

The major computation of algorithm is the computation of $\sigma(n)$ which is based on the complete integer factorization of n. Since at the present time, no efficient factoring algorithm has been found, then the algorithm cannot be preformed in deterministic polynomial time.

Calculation of odd perfect numbers

3.4.3. The simplest numerical method for searching of odd perfect numbers in a given interval $[A, B]$ can be obtained as an elementary modification of the previous algorithm.

- For odd n from A to B, find

$$\sigma(n) = \sigma(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+1}-1}{p_s-1};$$

- if $\sigma(n) = 2n$, then n is perfect.

However, there is a much better algorithm that will find an odd perfect number up to a given bound B or prove that there is none.

Let $N \le B$ be an odd perfect number with prime decomposition $N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Since N is perfect, then

$$2N = \sigma(N) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1}-1}{p_i-1},$$

and hence, we get the inequality

$$2 = \frac{\sigma(N)}{N} < \prod_{i=1}^{k} \frac{1}{1-p_i^{-1}} = \prod_{i=1}^{k} \frac{p_i}{p_i-1}.$$

So, N must be divisible by a reasonably small prime $p = o(\log B)$ which gives a finite number of possible prime powers p^α.

It is clear that if $p^\alpha || N$ (i.e., $p^\alpha | N$ but $p^{\alpha+1} \not| N$), then $\sigma(p^\alpha) | 2N$.

So, the factorization of $\sigma(p^\alpha)$ gives a number of primes which divide N. Proceeding in this way, more and more primes that divide N can be deduced, and hopefully, a contradiction to $N \leq B$ will be obtained.

In that way, Brent, Cohen, and te Riele have showed that

- *there are no odd perfect numbers less than* 10^{300}.

In 2012, Ochem and Rao proved that

- *there are no odd perfect numbers less than* 10^{1500}.

Algebraic assumption methods for perfect numbers and Mersenne primes

3.4.4. Due to the Euclid–Euler theorem, we have a one-to-one correspondence between the even perfect numbers and the Mersenne primes. Any even perfect number has the form $2^{k-1}(2^k - 1)$, where $2^k - 1$ is a prime, in fact a Mersenne prime, $M_p = 2^p - 1$, $p \in P$.

If we consider the set of Mersenne numbers $M_n = 2^n - 1$, $n \in \mathbb{N}$, in context of their primality, we are going to study only Mersenne numbers M_p with odd prime indexes p: otherwise, the situation becomes trivial.

So, the principal problem studied in connection with the even perfect numbers is that of the primality of numbers $M_p = 2^p - 1$ with odd prime p.

The most elementary and obvious method for finding the factors of a given number n is to test it for divisibility by primes less than $\sqrt{n}$; but if the given number is a large prime or has only large prime factors, the corresponding work is almost prohibitive.

One of the earliest used improvements on this method consists in determining certain properties of the prime factors of the numbers in consideration and then testing with only those primes which have this property.

Prime divisors of Mersenne numbers

3.4.5. In this section, we are going to prove that all prime divisors of Mersenne numbers with odd prime indexes are of the special form.

In fact, there exists the following divisibility property:

- *If* $q \in P$, $q \equiv \pm 1 (mod\, 8)$, *then* $q | M_{\frac{q-1}{2}}$.

□ It is easy to see that for any odd prime q, it holds that $q \equiv \pm 1 (mod\, 8)$ or $q \equiv \pm 3 (mod\, 8)$. If $q \equiv \pm 1 (mod\, 8)$, we get using the properties of the *Legendre symbol* (see Chapter 1, Section 1.5) that $(\frac{2}{q}) = 1$. So, by the *Euler's criterion*, it holds that

$$2^{\frac{q-1}{2}} \equiv 1 (mod\ q)$$

and $q | M_{\frac{q-1}{2}}$. □

For example, for $q = 23$, one has $\frac{q-1}{2} = 11$, and $23 | M_{11}$; for $q = 47$, one has $\frac{q-1}{2} = 23$, and $47 | M_{23}$.

On the other hand, one can start from $n = 11$; for $n = 11$, one has $q = 2n + 1 = 23$, and $23 | M_{11}$. So, M_{11} is composite; it is the first composite Mersenne number with prime index. Similarly, for $n = 23$, one has $q = 2p + 1 = 47$, and $47 | M_{23}$. So, M_{23} is composite. Therefore, we have proved the following important fact:

- *For* $p \in P$, $p \equiv -1 (mod\ 4)$, *if* $q = 2p + 1$ *is prime, then* M_p *is composite.*

□ For $p \equiv -1 (mod\ 4)$, we get $2p + 1 \equiv \pm 1 (mod\ 8)$; so, in the case of primality of $q = 2p - 1$, $q | M_p$, and so, M_p is composite. □

In particular, if $p = 11, 23, 83, 131, 179, 191, 239, 251$, then M_p is divisible by 23, 47, 167, 263, 359, 383, 479, 503, respectively.

3.4.6. A prime number p is called a *Sophie Germain prime* (named after the French mathematician Marie-Sophie Germain) if $2p + 1$ is also prime.

The number $2p + 1$ associated with a Sophie Germain prime p is called a *safe prime.*

So, we get a *property of compositeness of Mersenne numbers with prime index* $p \equiv -1 (mod\, 4)$:

- *Let* $p \in P$, $p \equiv -1 (mod\, 4)$, $p > 3$. *Then,* $M_p \in S$ *if* p *is a Sophie Germain prime; in fact, in this case,* M_p *is divisible by the associated safe prime* $2p + 1$.

The first Sophie Germain primes are 2, 3, 5, 11, 23, 29, 41, 53, 83, $89, \ldots$ (sequence A005384 in the OEIS). Hence, the first safe primes are 5, 7, 11, 23, 47, 59, 83, 107, 167, $179, \ldots$ (sequence A005385 in the OEIS).

The largest known Sophie Germain prime (as of 2021) is $137211941292195 \cdot 2^{171960} - 1$ (Járai *et al.*, 2006). It has 51780 digits.

3.4.7. One can show that any possible prime divisor of a given Mersenne number M_p with odd prime index p has the form $2pk + 1$:

- *If* $q, p \in P \backslash \{2\}$, *and* $q|M_p$, *then* $q = 2pk + 1$ *for some* $k \in \mathbb{N}$.

□ Indeed, if $q \in P$ and $q|M_p$, we have, due to the Fermat's little theorem, that

$$2^p \equiv 1 (mod\, q),$$

i.e., the multiplicative order $ord_q\, 2$ of 2 modulo q divides p: $ord_q\, 2|p$. As $ord_q\, 2 \neq 1$, it holds that $ord_q\, 2 = p$.

Therefore, by the properties of multiplicative order, we get that $p|(q - 1)$, i.e., $q \equiv 1 (mod\, p)$.

Obviously, $q \equiv 1 (mod\, 2)$. So, $q \equiv 1 (mod\, p)$, $q \equiv 1 (mod\, 2)$, and we obtain that $q \equiv 1 (mod\, 2p)$, i.e., $q = 2pk + 1$, $k \in \mathbb{N}$. □

3.4.8. It is easy to show that *any prime divisor* q *of a Mersenne number* M_p *with odd prime index* p *is equal to* ± 1 *modulo 8*:

- *If* $q, p \in P \backslash \{2\}$, *and* $q|M_p$, *then* $q \equiv \pm 1 (mod\, 8)$.

□ Consider $q \in P$, $q|M_p$. As $p \in P \backslash \{2\}$, then p is odd, i.e., $p = 2k + 1$. Hence, $q|(2^{2k+1} - 1)$, or $q|(2(2^k)^2 - 1)$, i.e.,

$$q| \left(2(2^k x)^2 - x^2 \right)$$

for any integer x.

As $gcd(2^k, q) = 1$, there exist integers x_0 and y_0 such that $2^k x_0 - qy_0 = 1$.

Therefore, $2^k x_0 = 1 + qy_0$. It means that

$$q| \left(2(1+qy_0)^2 - x_0^2\right)$$

or

$$q| \left((2(qy_0)^2 + 4qy_0) + (2 - x_0^2)\right).$$

As $q|(2(qy_0)^2 + 4qy_0)$, we get that $q|(2 - x_0^2)$.

Consider the decomposition of $\frac{x_0}{q}$ into a *continued fraction* (see Chapter 1, Section 1.6):

$$\frac{x_0}{q} = [a_0, a_1, \ldots, a_s] = a_0 + \cfrac{1}{a_1 + \frac{1}{\cdots + \frac{1}{a_s}}}.$$

Let $[a_0, a_1, \ldots, a_k] = \frac{P_k}{Q_k}$. Then,

$$1 = Q_0 \le Q_1 < Q_2 < \cdots < Q_s = q.$$

As $q > 1$, there exists an index n, such that $Q_n^2 < q < Q_{n+1}^2$. Then,

$$\left|\frac{x_0}{q} - \frac{P_n}{Q_n}\right| \le \frac{q^2}{Q_{n+1}^2} < q.$$

Therefore,

$$0 \le (x_0 Q_n - qP_n)^2 \le \frac{q^2}{Q_{n+1}^2} < q,$$

and we get that

$$-2q < -2Q_n^2 \le (x_0Q_n - qP_n)^2 - 2Q_n^2 = (x_0^2 - 2)Q_n^2 + qM < q - 2Q_n^2 < q.$$

As $q|(2 - x_0^2)$, we have that $(x_0^2 - 2)Q_n^2 + qM$ is divisible by q, i.e., $(x_0Q_n - qP_n)^2 - 2Q_n^2$ is divisible by q. But

$$-2q < (x_0Q_n - qP_n)^2 - 2Q_n^2 < q.$$

So, $(x_0Q_n - qP_n)^2 - 2Q_n^2$ can only take values 0 or $-q$.

In the first case, we obtain a contradiction, as we have $2 = t^2$, where $t = \frac{x_0Q_n - qP_n}{Q_n}$ is a rational number.

In the second case, we get the representation

$$q = 2x^2 - y^2, \quad \text{where} \quad x = Q_n, \quad y = x_0Q_n = qP_n.$$

In this situation, y should be odd: $y = 2k + 1$. Therefore,

$$y^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1 \equiv 1(mod\,8).$$

If x is odd, then $2x^2 \equiv 2(mod\,8)$, and $q \equiv 1(mod\,8)$.

If x is even, then $2x^2 \equiv 0(mod\,8)$, and $q \equiv -1(mod\,8)$. □

3.4.9. Using the information above, we can now get a representation of any possible prime divisor of the Mersenne number M_p with odd prime index p:

- *If* $q, p \in P\backslash\{2\}$, $q|M_p$, *and* $p = 4t \mp 1$, *then* $q \in \{8pk + 1, 8pk + 1 \pm 2p\}$.

□ By the last two properties, we have that $q = 2pt + 1$ and $q \equiv \pm 1(mod\,8)$.

I. If $q = 2pt + 1$ and $q \equiv 1(mod\,8)$, then

$$2pt \equiv 0(mod\,8),\ pt \equiv 0(mod\,4),\ t \equiv 0(mod\,4).$$

So, we get that $q = 8pk + 1$.

II. If $q = 2pt + 1$ and $q \equiv -1(mod\,8)$, then

$$2pt \equiv -2(mod\,8),\ pt \equiv -1(mod\,4).$$

If $p \equiv 1(mod\,4)$, then $t \equiv -1(mod\,4)$, and $q = 8pk + 1 - 2p$.

Otherwise, $p \equiv -1(mod\,4)$, $t \equiv 1(mod\,4)$, and $q = 8pk + 1 + 2p$. □

3.4.10. L. Euler (1771) proved that M_{31} is prime by testing prime numbers of the form $248n + 1$, $248n + 63$ below 46339 as possible factors of M_{31} (there are only 84 such primes).

But even a reduced set of possible factors grows too large as M_p increases.

Lucas–Lehmer test

The other method for testing primality of Mersenne numbers is the *Lucas–Lehmer test.*

3.4.11. The theory for this test was initiated by É. Lucas in the late 1870s. É. Lucas studied *Fibonacci numbers*, i.e., the positive integers u_n such that $u_1 = 1$, $u_2 = 1$, and

$$u_{n+2} = u_n + u_{n+1}$$

for any $n \in \mathbb{N}$. While studying the Fibonacci numbers, É. Lucas discovered the following fact:

- *If* $n \equiv \pm 3 (mod\, 10)$ *and* n *is a proper divisor of* u_{n+1} *(i.e.,* $n | u_{n+1}$ *and* $n \not| u_i$ *for* $i < n+1$*), then* n *is a prime; if* $n \equiv \pm 1 (mod\, 10)$ *and* n *is a proper divisor of* u_{n-1} *(i.e.,* $n | u_{n-1}$*, and* $n \not| u_i$ *for* $i < n-1$*), then* n *is a prime.*

Using this approach, É. Lucas proved the primality of M_{127} in 1876. He wrote: "...I have proved that number $A = 2^{127} - 1$ is prime. Indeed, the number A is of the form $10k - 3$, and I have verified that u_k is never divisible by A for $k = 2^n$, except for $n = 127$."

So, the primality of the Mersenne number

$$M_{127} = 2^{127} - 1 = 170141183460 \ldots 715884105727$$

was proven in 1876. It was the last case of "hand" checking of the primality of a Mersenne number.

After É. Lucas formulated the theory, D. H. Lehmer, in 1930, simplified the primality test of Lucas.

Using a new version of the test, D. H. Lehmer managed to prove that M_{257} is a composite number.

3.4.12. In this section, we consider the proof of the *Lucas–Lehmer primality test.*

Theorem (Lucas–Lehmer test). *A number* M_p*,* p *being an odd prime, is a prime if and only if it is a divisor of the* $(p-1)$*th term of the sequence* $S_1, S_2, \ldots, S_{p-1}$*, where* $S_1 = 4$ *and* $S_{k+1} = S_k^2 - 2$.

□ Let $a = 1 + \sqrt{3}$ and $b = 1 - \sqrt{3}$, i.e., $a + b = 2$ and $ab = -2$. Let $u_r = \frac{a^r - b^r}{a - b}$ and $v_r = a^r + b^r$.

I. It is easy to check that *there exist the following identities*:

1. $2u_{r+s} = u_r v_s + v_r u_s$;
2. $u_s v_r - u_r v_s = (-2)^{s+1} u_{r-s}$;
3. $v_r v_s + 12 u_r u_s = 2v_{r+s}$;
4. $u_r v_r = u_{2r}$;
5. $v_r^2 + (-2)^{r+1} = n_{2r}$;
6. $v_r^2 - 12u_r^2 = (-2)^{r+2}$.

For example,

$$\begin{aligned} u_r v_s + v_r u_s &= \frac{a^r - b^r}{a-b}(a^s + b^s) + \frac{a^s - b^s}{a-b}(a^r + b^r) \\ &= \frac{2a^{r+s} - 2b^{r+s} + a^r b^s - b^r a^s + a^s b^r - a^r b^s}{a-b} \\ &= 2\frac{a^{r+s} - b^{r+s}}{a-b} = 2u_{r+s}. \end{aligned}$$

II. It holds that *for a given prime $p > 3$, we have the following congruences*:

$$u_p \equiv \left(\frac{3}{p}\right)(mod\, p) \text{ and } v_p \equiv 2(mod\, p).$$

In fact,

$$\begin{aligned} u_p &= \frac{(1+\sqrt{3})^p - (1-\sqrt{3})^p}{2\sqrt{3}} \\ &= \frac{1}{2\sqrt{2}}\left(2\binom{p}{1}\sqrt{3} + 2\binom{p}{2}(\sqrt{3})^3 + \cdots + 2\binom{p}{p}(\sqrt{3})^p\right) \\ &= \binom{p}{1} + 3\binom{p}{3} + \cdots + \binom{p}{p}3^{\frac{p-1}{2}} \equiv 3^{\frac{p-1}{2}} \\ &= \left(\frac{3}{p}\right)(mod\ p), \end{aligned}$$

as binomial coefficients $\binom{p}{k} \equiv 0(mod\, p)$ for any $k \in [1, p-1]$. In a similar way,

$$\begin{aligned} v_p &= \left(1+\sqrt{3}\right)^p + \left(1-\sqrt{3}\right)^p \\ &= 2 + 2\binom{p}{2}\left(\sqrt{3}\right)^2 + \cdots + 2\binom{p}{p-1}\left(\sqrt{3}\right)^{\frac{p-1}{2}} \equiv 2(mod\ p). \end{aligned}$$

III. Let p be a prime and $p > 3$. Let $p|u_w$, but p does not divide u_r with $r < w$. Then, the number $w = w(p)$ is called *rang* of p.

We can prove that $p|u_r$ *if and only if* $w|r$, *where* p *is a prime,* $p > 3$, *and* w *is the rang of* p.

In fact, let $X_p = \{r : u_r \equiv 0(mod\, p)\}$. Using the first and second identities of **I**, we obtain the following fact:

If $u_r \equiv 0(mod\, p)$ *and* $u_s \equiv 0(mod\, p)$, *then* $u_{r\pm s} \equiv 0(mod\, p)$.

If w is the least number from the set X_p and $r \in X_p$, then consecutive subtractions give $r - kw = 0$, i.e., $w|r$.

IV. We are going to prove that $w \leq p+1$, *where* p *is a prime,* $p > 3$ *and* w *is the rang of* p.

For a proof of this fact, it is sufficient to show that $p|u_{p-1}u_{p+1}$.

Using the first and second identities of **II**, the values $r = p$ and $s = 1$.

Then, as $u_1 = 1$ and $v_1 = 2$, we obtain that

$$2u_{p+1} = v_p + 2u_p, \quad \text{and} \quad 4u_{p-1} = v_p - 2u_p.$$

Therefore, one has, using **II**, that

$$8u_{p+1}u_{p-1} = v_p^2 - 4u_p^2 = 4 - 4(\pm 1)^2 \equiv 0(mod\ p).$$

V. Let us prove now that $v_{2^k} = 2^{2^{k-1}}S_k$, i.e., $M_p|S_k$ *if and only if* $M_p|v_{2^k}$.

In fact, for $k = 1$, one has that $v_2 = 8 = 2S_1$. Going from k to $k+1$, we obtain, using the fifth identity of **I** with $r = 2^k$, that

$$v_{2^{k+1}} = v_{2^k}^2 - 2^{2^k+1} = (2^{2^{k-1}}S_k)^2 - 2^{2^k+1} = 2^{2^k}(S_k^2 - 2) = 2^{2^k}S_{k+1}.$$

VI. Consider *the proof of the first proposition of the theorem: If* $M_p \in P$, *then* $M_p|S_{p-1}$.

Let $M_p \in P$. It is sufficient to show that

$$M_p|v_{2^{p-1}} = v_{\frac{M_p+1}{2}}.$$

Using the fifth identity of **I** with $r = \frac{M_p+1}{2}$, we obtain that

$$v_{M_p+1} = v^2_{\frac{M_p+1}{2}} - 4 \cdot 2^{\frac{M_p-1}{2}}.$$

As $M_p \in P$, and as for prime $p > 3$, we have $M_p = 2^p - 1 \equiv -1(mod\, 8)$, then $(\frac{2}{M_p}) = 1$, i.e., $2^{\frac{M_p-1}{2}} \equiv 1(mod\, p)$. Therefore,

$$v_{M_p+1} \equiv v^2_{\frac{M_p+1}{2}} - 4(mod\ p).$$

On the other hand, using the third identity of **I** with $r = M_p$ and $s = 1$, we obtain that

$$2v_{M_p+1} = 2v_{M_p} + 12u_{M_p}$$

(as $v_1 = 2$ and $u_1 = 1$). Now, noting that $M_p \equiv -1(mod\ 4)$ and $M_p \equiv 1(mod\ 3)$, i.e., that

$$\left(\frac{3}{M_p}\right) = -\left(\frac{M_p}{3}\right) = -\left(\frac{1}{3}\right) = -1,$$

we obtain using **II** that

$$v_{M_p+1} \equiv v_{M_p} + 6u_{M_p} \equiv 2 + 6\left(\frac{3}{M_p}\right) \equiv 2 - 6 \equiv -4(mod\ M_p).$$

Therefore,

$$v^2_{\frac{M_p+1}{2}} \equiv 0(mod\ M_p).$$

VII. Consider *the proof of the second proposition of the theorem: If $M_n|S_{n-1}$, then M_n is a prime number.*

Let $M_n|S_{n-1}$, i.e., $M_n|v_{2^{n-1}}$. Let $p|M_n$. As for $k > 1$, any $S_k \equiv -1(mod\, 3)$, then $p > 3$. Let w be the rang of p. Using the fourth identity of **I** with $r = 2^{n-1}$, we obtain that

$$M_n|u_{2^n} = u_{2^{n-1}}v_{2^{n-1}}.$$

Therefore, one has that $p|u_{2^n}$, i.e., by **III**, that $w|2^n$.

It is easy to see that $w = 2^n$. In fact, if $w < 2^n$, then $p|u_{2^{n-1}}$, and using the last identity of **I** with $r = 2^{n-1}$, we obtain that

$$p|\left(v^2_{2^{n-1}} - 12u^2_{2^{n-1}}\right) = (-2)^{2^{n-1}+2},$$

a contradiction.

But, by **IV**, we have that $w \leq p+1$. Therefore, one has that $p \geq w-1 = 2^n - 1 = M_n$, where p is a prime dividing M_n, i.e., we obtain that $p = M_n$. □

3.4.13. Practical algorithm of computation using the Lucas–Lehmer test works as follows.

Let $M_p = 2^p - 1$ be a Mersenne number to test with p an odd prime. (The primality of p can be efficiently checked with a simple algorithm like trial division since p is exponentially smaller than M_p.) Define a sequence $\{S_i\}$: $S_1 = 4$ and $S_{i+1} = S_i^2 - 2$ for any positive integer i.

The first terms of this sequence are 4, 14, 194, 37634, 1416317954, 2005956546822746114,... (sequence A003010 in the OEIS).

Then, M_p is prime if and only if

$$S_{p-1} \equiv 0 (mod\ M_p).$$

The number S_{p-1} modulo M_p is called the *Lucas–Lehmer residue* of p.

For example, the Mersenne number $M_3 = 2^3 - 1 = 7$ is prime, as $S_1 = 4$ and $S_2 = 4^2 - 2 = 14 \equiv 0(mod\ 7)$.

The Mersenne number $M_5 = 2^5 - 1 = 31$ is prime, as $S_1 = 4$, $S_2 \equiv 4^2 - 2 \equiv 14(mod\ 31)$; $S_3 \equiv 14^2 - 2 \equiv 8(mod\ 31)$; $S_4 \equiv 8^2 - 2 \equiv 0(mod\ 31)$.

On the other hand, in order to check the primality of $M_{11} = 2^{11} - 1 = 2047$, we obtain the sequence $S_1, \ldots, S_{10}$ modulo 2047: $S_1 \equiv 4(mod\ 2047)$; $S_2 \equiv 4^2 - 2 \equiv 14(mod\ 2047)$; $S_3 \equiv 14^2 - 2 \equiv 194(mod\ 2047)$; $S_4 \equiv 194^2 - 2 \equiv 788(mod\ 2047)$; $S_5 \equiv 788^2 - 2 \equiv 701(mod\ 2047)$; $S_6 \equiv 701^2 - 2 \equiv 119(mod\ 2047)$; $S_7 \equiv 119^2 - 2 \equiv 1877(mod\ 2047)$; $S_8 \equiv 1877^2 - 2 \equiv 240(mod\ 2047)$; $S_9 \equiv 240^2 - 2 \equiv 282(mod\ 2047)$; $S_{10} \equiv 282^2 - 2 \equiv 1736(mod\ 2047)$. So, $S_{10} \not\equiv 0(mod\ 2047)$, and hence, M_{11} is composite.

In the Lucas–Lehmer test, the starting values S_1 other than 4 are possible. In fact, the possible starting values for S_1 are 4, 10, 52, 724, 970, 10084, 95050, 140452, 1956244, 9313930,... (sequence A018844 in the OEIS).

The Lucas–Lehmer residue calculated with these alternative starting values will still be zero if M_p is a Mersenne prime. However, the terms of the sequence will be different and a non-zero Lucas–Lehmer residue for composite M_p will have a different numerical value from the non-zero value calculated when $S_1 = 4$.

Starting values such as 4 and 10 are universal, that is, they are valid for all (or nearly all) p. In fact, there are infinitely many additional universal starting values.

However, some other starting values are only valid for a subset of all possible p. For example, $S_0 = 3$ can be used if $p \equiv 3(mod\ 4)$. This starting value was often used in the era of hand computation, including by É. Lucas in proving the primality of M_{127}.

3.4.14. The Lucas–Lehmer test happens to be ideally suited for binary computers, as the computation of S_k does not involve division and can be done using only multiplication (rotation) and addition, which binary computers do quickly.

The sequence S_n is computed modulo $M_p = 2^p - 1$ to save time. Taking each S_k modulo M_p is easy in binary too because M_p is a string of the unities in binary.

After É. Lucas, the next larger Mersenne prime was discovered in 1952 by Raphael M. Robinson with computer assistance. It was

$$M_{521} = 686479766013 \ldots 291115057151.$$

Today the Lucas–Lehmer test is the primality test used by the GIMPS to locate large primes. This search has been successful in locating many of the largest primes known to date.

As of 2021, there exist 51 known Mersenne prime. It means that there exist 51 known (even) perfect numbers. The first, second, third, and fourth perfect numbers are, respectively,

$$6 = 2^1(2^2 - 1) = 2 \cdot M_2;\ 28 = 2^2(2^3 - 1) = 2^2 \cdot M_3;$$
$$496 = 2^4(2^5 - 1) = 2^4 \cdot M_5;\ 8128 = 2^6(2^7 - 1) - 2^6 \cdot M_7.$$

They correspond to the first, second, third, and fourth Mersenne primes, $M_2 = 3$. $M_3 = 7$, $M_5 = 31$, and $M_7 = 127$, respectively.

The 48th perfect number is

$$2^{57885160}(2^{57885161} - 1) = 2^{257885160} \cdot M_{57885161}(34850339 \ \ \text{digits}).$$

It corresponds to the 48th Mersenne prime $M_{57885161} = 581887\ldots 285951$ (17425170 digits).

The three biggest known even perfect numbers are

$$2^{74207280}(2^{74207281}-1) = 2^{74207280}\cdot M_{274207281}(44677235 \ \text{ digits});$$
$$2^{77232916}(2^{77232917}-1) = 2^{77232916}\cdot M_{277232917}(46498850 \ \text{ digits});$$
$$2^{82589932}(2^{82589933}-1) = 2^{82589932}\cdot M_{282589933}(49724095 \ \text{ digits}).$$

They correspond to the Mersenne primes $M_{74207281} = 300376\ldots 436351$ (22338618 digits), $M_{77232917} = 467333\ldots 179071$ (23249425 digits), and $M_{82589933} = 148894\ldots 902591$ (24862048 digits). However, it has not been verified whether any undiscovered Mersenne primes exist between the 48th Mersenne prime $M_{57885161}$ and the biggest known (in fact, 51st known) Mersenne prime $M_{8258993}$. So, the ranks 49, 50, and 51 may change if smaller ones are discovered.

Mersenne numbers and prime numbers records

3.4.15. At present, the search for new large Mersenne primes is a important part of pure mathematics and computer science. In recent years, several distributed computing projects, including *PrimeGrid*, *GIMPS*, *Fermat Search*, *Twin Prime Search*, etc. have been hunting for very large prime numbers while also aiming to solve long-standing mathematical conjectures.

In the following table, we list the 20 largest known primes.

The 20 largest known primes

	Prime	Number of digits	Year	Comment
1	$2^{82589933}-1$	24862048	2018	51st (?) Mersenne prime
2	$2^{77232917}-1$	23249425	2018	50th (?) Mersenne prime
3	$2^{74207281}-1$	22338618	2016	49th (?) Mersenne prime
4	$2^{57885161}-1$	17425170	2013	48th (?) Mersenne prime
5	$2^{43112609}-1$	12978189	2008	47th Mersenne prime
6	$2^{42643801}-1$	12837064	2009	46th Mersenne prime
7	$2^{37156667}-1$	11185272	2008	45th Mersenne prime

(*Continued*)

	Prime	Number of digits	Year	Comment
8	$2^{32582657}-1$	9808358	2006	44th Mersenne prime
9	$10223 \cdot 2^{31172165}+1$	9383761	2016	
10	$2^{30402457}-1$	9152052	2005	43rd Mersenne prime
11	$2^{25964951}-1$	7816230	2005	42nd Mersenne prime
12	$2^{24036583}-1$	7235733	2004	41st Mersenne prime
13	$2^{20996011}-1$	6320430	2003	40th Mersenne prime
14	$1059094^{1048576}+1$	6317602	2018	Generalized Fermat prime
15	$919444^{1048576}+1$	6253210	2017	Generalized Fermat prime
16	$168451 \cdot 2^{19375200}+1$	5832522	2017	
17	$7 \cdot 2^{18233956}+1$	5488969	2020	Divides Fermat number $F_{18233954}$
18	$123447^{1048576} - 123447^{524288}+1$	5338805	2017	Generalized unique prime
19	$7 \cdot 6^{6772401}+1$	5269954	2019	
20	$8508301 \cdot 2^{17016603}-1$	5122515	2018	

3.4.16. It is easy to see that the largest known prime has almost always been a Mersenne prime.

Why? Because the way the largest numbers N are proven prime is based on the factorization of either $N+1$ or $N-1$. For Mersenne numbers, the factorization of $N+1$ is as trivial as possible; it is a power of two.

At present, there are few practical uses for this new large primes, prompting some to ask “why search for these large primes?”

Those same doubts existed a few decades ago until important cryptography algorithms were developed based on prime numbers.

5.4.3. The *GIMPS* is a collaborative project of volunteers who use freely available software to search for Mersenne prime numbers.

GIMPS is said to be one of the first large-scale distributed computing projects over the Internet for research purposes.

It has had a virtual lock on the largest known prime because its excellent free software is easy to install and maintain, requiring little of the user.

GIMPS was founded in early 1996 by G. Woltman to discover new world-record-size Mersenne primes.

GIMPS is registered as *Mersenne Research, Inc.* with S. Kurowski as Executive Vice President and board director.

The name for the project was coined by L. Welsh, one of its earlier searchers and the co-discoverer of the 29th Mersenne prime.

Within a few months, several dozen people had joined and over a thousand by the end of the first year.

J. Armengaud, a participant, discovered the primality of $M_{1398269}$ on November 13, 1996.

In 1997, S. Kurowski enabled GIMPS to automatically harness the power of thousands of ordinary computers to search for these "needles in a haystack."

Most GIMPS members join the search for the thrill of possibly discovering a record-setting, rare, and historic new Mersenne prime.

3.4.17. As of 2021, the project has found a total of 17 Mersenne primes, 15 of which were the largest known prime numbers at their respective times of discovery.

In 1996, J. Armengaud *et al.* discovered the 35th Mersenne prime $M_{1398269}$ in France.

In 1999, Nayan N. Hajratwala discovered the first known million-digit prime number using software written by G. Woltman and the distributed computing technology and services of Kurowski's company.

This prime number, $2^{6972593} - 1$, is the 38th Mersenne prime. It contains 2098960 digits.

Nayan Hajratwala used a Pentium II IBM Aptiva computer running part time for 111 days to prove the number prime.

Running uninterrupted it would take about three weeks to test the primality of this number.

There are several prizes offered by the Electronic Frontier Foundation for record primes.

This record passed one million digits in 1999, earning a USD 50,000 prize.

In 2008, the record passed ten million digits (12978189 digits of $M_{43112609}$, the 47th Mersenne prime), earning a USD 100,000 prize and a Cooperative Computing Award from the Electronic Frontier

Foundation. *Time* (an American weekly news magazine) called it the 29th top invention of 2008.

Both the USD 50,000 and the USD 100,000 prizes were won through participation in the GIMPS.

As of 2021, the largest known prime is $2^{82589933} - 1$ ($M_{82589933}$). It has 24862048 digits. It was discovered in 2018 by P. Laroche, one of the thousands of volunteers using free GIMPS software available at *www.mersenne.org/download/*.

The new prime number $M_{82589933}$ is calculated by multiplying together 82589933 twos and then subtracting one.

It is more than one and a half million digits larger than the previous record prime number $2^{74207281} - 1$, $M_{14207281}$ (having 23249425 digits).

It is only the 51st known Mersenne prime ever discovered, each increasingly more difficult to find.

For many years, P. Laroche had used GIMPS software as a free "stress test" for his computer builds. During that time, he started prime hunting on his media server to "give back" to the project. After less than four months and on just his fourth try, he discovered the new prime number.

By way of comparison, some GIMPS participants have searched for more than 20 years with tens of thousands of attempts but no success, thus proving that even the "little guy" can compete against those with lots of computing resources.

The primality proof took 12 days of non-stop computing. To prove there were no errors in the prime discovery process, the new prime was independently verified using three different programs on three different hardware configurations.

The number $M_{82589933}$ has 24862048 decimal digits. To help visualize the size of this number, if it were to be saved to disk, the resulting text file would be nearly 25 megabytes long (most books in plain text format clock in under two megabytes). A standard word processor layout (50 lines per page, 75 digits per line) would require 6629 pages to display it.

GIMPS is also coordinating its long-range search efforts for primes of 100 million digits and larger and will split the Electronic Frontier

Foundation's USD 150,000 prize with a winning participant. Additional prize is being offered for the first prime number found with at least one billion digits.

3.4.18. GIMPS has also been extremely lucky over the last 15 years. The largest known prime $M_{82589933}$ is GIMPS' 12th prime discovery between $2^{20000000} - 1$ and $2^{85000000} - 1$, triple the expected number of new primes in this interval.

One reason to search for new primes is to match actual results with expected results. This anomaly is not necessarily evidence that existing theories on the distribution of Mersenne primes is incorrect. However, if the trend continues it may be worth further investigation.

On December 4, 2020, the project passed a major milestone after all exponents below 100 million were checked at least once.

3.4.19. There is a unique history to the arithmetic algorithms underlying the GIMPS project.

In the early 1990s, R. Crandall, Apple Distinguished Scientist, discovered ways to double the speed of what are called *convolutions*, essentially big multiplication operations.

The method is applicable not only to prime searching but other aspects of computation.

During that work, he also patented the *fast elliptic encryption system*, now owned by Apple Computer, which uses Mersenne primes to quickly encrypt and decrypt messages.

G. Woltman implemented Crandall's algorithm in assembly language, thereby producing a prime-search program of unprecedented efficiency.

In general, GIMPS project relies primarily on the *Lucas–Lehmer primality test*, as it is an algorithm that is both specialized for testing Mersenne primes and particularly efficient on binary computer architectures.

There is also a *trial division* phase used to rapidly eliminate many Mersenne numbers with small factors.

Pollard's $(p-1)$ *algorithm* is also used to search for smooth factors.

In 2017, GIMPS adopted the *Fermat primality test* as an alternative option for primality testing.

3.4.20. The search for more Mersenne primes is already under way. There may be smaller, as yet undiscovered, Mersenne primes, and there almost certainly are larger Mersenne primes waiting to be found.

Anyone with a reasonably powerful personal computer can join GIMPS and become a big prime hunter and possibly earn a cash award for research discovery.

All the necessary software can be downloaded for free at www.mersenne.org/download/.

For the other proofs of the Lucas–Lehmer theorem, additional information and useful references, see, for example, in [Buch09], [Cohn65], [DeKo13], [DeKo18], [Ribe89], [Ribe96], [SlPl95], [GIMPS20], [Prim22], [Sloa22], and [Wiki22].

Exercises

1. Check the following congruences:

   (a) $M_n \equiv 1 (mod\ 2)$ for $n \geq 1$;
   (b) $M_n \equiv 3 (mod\ 4)$ for $n \geq 2$;
   (c) $M_n \equiv 7 (mod\ 8)$ for $n \geq 3$;
   (d) $M_n \equiv 15 (mod\ 16)$ for $n \geq 4$.

2. Prove the following properties:

   (a) $3|M_n \Leftrightarrow 2|n$;
   (b) $5|M_n \Leftrightarrow 4|n$;
   (c) $7|M_n \Leftrightarrow 3|n$;
   (d) $11|M_n \Leftrightarrow 10|n$;
   (e) $13|M_n \Leftrightarrow 12|n$;
   (f) $17|M_n \Leftrightarrow 8|n$;
   (g) $19|M_n \Leftrightarrow 18|n$;
   (h) $23|M_n \Leftrightarrow 11|n$.

3. Prove that $u_0+u_1+u_2+\cdots+u_n = u_{n+2}-1$; $u_1+u_3+\cdots+u_{2n-1} = u_{2n}$; $u_2+u_4+\cdots+u_{2n} = u_{2n+1}-1$; $u_1^2+u_2^2+\cdots+u_n^2 = u_n \cdot u_{n+1}$; $u_1u_2 + u_2u_3 + \cdots + u_{2n-1}u_{2n} = u_{2n}^2$; $u_1u_2 + \cdots + u_{2n}u_{2n+1} = u_{2n+1}^2 - 1$.
4. Let $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$; prove the *Binet's formula* $u_n = \frac{\alpha^n-\beta^n}{\sqrt{5}}$, $n \in \mathbb{N}$.
5. Let $\alpha = 2+\sqrt{3}$ and $\beta = 2-\sqrt{3}$; prove that $S_{i+1} = \alpha^{2^i} + \beta^{2^i}$ for any $i \geq 0$.

6. Prove the Lucas–Lehmer theorem using the numbers $\alpha = 2 + \sqrt{3}$ and $\beta = 2 - \sqrt{3}$.
7. Prove the primality of $M_7 = 2^7 - 1 = 127$ (of $M_{13} = 2^{13} - 1 = 8191$; of $M_{17} = 2^{17} - 1 = 131071$) using the Lucas–Lehmer primality test.
8. Prove the primality of $M_3 = 2^3 - 1 = 7$ (of $M_5 = 2^5 - 1 = 31$; of $M_7 = 2^7 - 1 = 127$) using the Lucas–Lehmer primality test with $S_1 = 10$.
9. Using the table of Mersenne primes, find the first Mersenne titanic prime (a prime number of at least 1000 decimal digits); the first Mersenne gigantic prime (a prime number with at least 10000 decimal digits); the first Mersenne megaprime (a prime number with at least one million decimal digits).
10. Find the set of all possible prime divisors of M_p, $p = 7, 13, 19$. Using this information, prove that M_p is prime.
11. Let p be a Sophie Germain prime, $p > 3$. Prove that $p \equiv 2 (mod\ 3)$. Let q be a safe prime, $q > 7$. Prove that $q \equiv 3 (mod\ 4)$, $q \equiv 5 (mod\ 6)$, $q \equiv 11 (mod\ 12)$. Prove that any safe prime $q > 7$ divides $3^{\frac{q-1}{2}-1}$.
12. Find several sequences $\{p, 2p+1, 2(2p+1)+1, \ldots\}$ in which all of the numbers are primes (such sequence is called a *Cunningham chain* of the first kind).

3.5. Perfect Numbers in the Family of Special Numbers

Perfect, abundant, and deficient numbers

3.5.1. The sum of proper divisors gives various other kinds of numbers.

Numbers whose sum is less than the number itself are called *deficient*, and whose sum is greater than the number, *abundant*. These terms, together with *perfect* itself, come from Greek numerology. In fact, the positive integers were first classified as either deficient, perfect, or abundant by Nicomachus in his *Introductio Arithmetica* (circa AD 100).

So, we can characterize a positive integer number using aliquot sum function $s(n)$ or, equivalently, sigma function $\sigma(n)$. If $s(n) = n$ (or $\sigma(n) = 2n$), we get perfect numbers. If $s(n) < n$ (or $\sigma(n) < 2n$), we get deficient numbers. If $s(n) > n$ (or $\sigma(n) > 2n$), we get abundant numbers.

Moreover, using the function $s(n)$ and $\sigma(n)$, we can define other classes of special numbers such that *highly abundant numbers*, for which it holds that $\sigma(k) < \sigma(n)$ for any $k < n$, *superabundant numbers*, for which $\frac{\sigma(k)}{k} < \frac{\sigma(n)}{n}$ for any $k < n$, and *colossally abundant numbers*, for which there exists an $\epsilon > 0$ such that $\frac{\sigma(n)}{n^{1+\epsilon}} \geq \frac{\sigma(k)}{k^{1+\epsilon}}$ for all $k > 1$.

In this section, we consider the main properties of these (and other) classes of numbers as well as their connections with perfect numbers.

3.5.2. A *deficient number* (or *defective number*) is a number n for which the sum of divisors of n is less than $2n$:

$$\sigma(n) < n.$$

Equivalently, it is a number for which the sum of proper divisors (i.e., aliquot sum) is less than n:

$$s(n) < n.$$

The value $2n - \sigma(n)$ is called the *deficiency*. In terms of the aliquot sum $s(n)$, the deficiency is $n - s(n)$.

For example, the positive integer divisors of 8 are 1, 2, 4, and 8, and their sum 15 is less than $16 = 2 \cdot 8$, so 8 is deficient (equivalently, the proper divisors of 8 are 1, 2, and 4, and their sum 7 is less than 8, so 8 is deficient). Its deficiency is $2 \cdot 8 - 15 = 1$.

As for the number 21, its positive integer divisors are 1, 3, 7, and 21, and their sum is 32. Because 32 is less than $42 = 2 \cdot 21$, the number 21 is deficient (equivalently, the proper divisors of 21 are 1, 3, and 7, and their sum 11 is less 21, so 21 is deficient). Its deficiency is $2 \cdot 21 - 32 = 10$.

The first few deficient numbers are 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, ... (sequence A005100 in the OEIS).

Since the aliquot sums of prime numbers equal 1, *all prime numbers are deficient*:

- *If* $p \in P$, *then* $\sigma(p) < 2p$.

□ In fact, $\sigma(p) = p + 1 < 2p$ for any prime p, which is obviously greater than 1. □

More generally, *all prime powers* p^k, $k \in \mathbb{N}$, *are deficient*:

- *If* $p \in P$, $k \in \mathbb{N}$, *then* $\sigma(p^k) < 2p^k$.

□ Because the only divisors of p^k are $1, p, p^2, \ldots, p^{k-1}, p^k$, which sum to $\frac{p^k-1}{p-1} + p^k$, which is at most $2p^k - 1$, we get $\sigma(p^k) < 2p^k$. □

Moreover, *the product of two primes except* $2 \cdot 3$ *is deficient*:

- *If* $p, q \in P$ *and* $pq \neq 6$, *then* $\sigma(pq) < 2pq$.

□ In this case, $\sigma(pq) = pq + p + q + 1 < 2pq$. □

In fact, *all odd numbers with one or two distinct prime factors are deficient.*

□ For example, $\sigma(75) = \sigma(3 \cdot 5^2) = 4 \cdot 31 = 124 < 150 = 2 \cdot 75$. □

It follows that

- *there are infinitely many deficient numbers, in particular, infinitely many odd deficient numbers as well as infinitely many even deficient numbers.*

□ In order to prove this proposition, one can consider the infinite set of primes, or for a given prime $p > 2$, the infinite set $p^k, k = 1, 2, 3, \ldots$, of its positive integer powers. All such numbers are deficient.

For $p = 2$, we get an important special case of an infinite set $2^k, k = 1, 2, 3, \ldots$ of even deficient numbers: for 2^k, its proper divisors are $1, 2, 2^2, \ldots, 2^{k-1}$, which sum to $2^k - 1$:

$$1 + 2 + 4 + 8 + \cdots + 2^{k-1} = 2^k - 1.$$

So, $s(2^k) = 2^k - 1 < 2^k$. □

It is easy to show that

- *all positive integer divisors of deficient numbers are deficient.*

Moreover,

- *all proper divisors of perfect numbers are deficient.*

□ In fact, let $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, $m = p_1^{\beta_s} \cdot \ldots \cdot p_s^{\beta_s}$, where α_i and β_i are non-negative integers; let kn be deficient or perfect, i.e.,

$$\sigma(kn) \leq 2kn;$$

then for $k > 1$, it holds that

$$\begin{aligned} k\sigma(n) &= \left(p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}\right) \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+1} - 1}{p_s - 1} \\ &< \left(p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}\right) \cdot \frac{p_1^{\alpha_1+1} - p_1^{-\beta_1}}{p_1 - 1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+1} - p_s^{-\beta_s}}{p_s - 1} \\ &= \frac{p_1^{\alpha_1+\beta_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+\beta_s+1} - 1}{p_s - 1} = \sigma(kn) \leq 2kn, \end{aligned}$$

i.e., we have that

$$\sigma(n) < 2n,$$

and n, which is, for $k > 1$, a proper divisor of kn, is deficient. □

It is proven (Sándor *et al.*, 2006) that

- *there exists at least one deficient number in the interval* $[n, n + (\log n)^2]$ *for all sufficiently large* n.

3.5.3. An *abundant number* (or *excessive number*) is a number n for which the sum of divisors of n is greater than $2n$:

$$\sigma(n) > n.$$

Equivalently, it is a number for which the sum of proper divisors (i.e., aliquot sum) is greater than n:

$$s(n) > n.$$

The value $\sigma(n) - 2n$ is called the *abundance*. In terms of the aliquot sum $s(n)$, the abundance is $s(n) - n$.

For example, the positive integer divisors of $12 = 2^2 \cdot 3$ are 1, 2, 3, 4, 6, and 12, and their sum 28 is greater than $24 = 2 \cdot 12$, so 12 is an abundant number and, in fact, the first abundant number (equivalently, the proper divisors of 12 are 1, 2, 3, 4, and 6, and their sum 16 is greater than 12, so 12 is abundant). Its abundance is $28 - 2 \cdot 12 = 4$.

As for the number $945 = 3^3 \cdot 5 \cdot 7$, its positive integer divisors are 1, 3, 5, 7, 9, 15, 21, 27, 35, 45, 63, 105, 135, 189, 315, and 945, and their sum is 1920. Because 1920 is less than $1890 = 2 \cdot 945$, the number 945 is an abundant number and, in fact, the first odd abundant number (equivalently, the proper divisors of 945 are 1, 3, 5, 7, 9, 15, 21, 27, 35, 45, 63, 105, 135, 189, and 315, and their sum 975 is greater than 945, so 945 is abundant). Its abundance is $1920 - 2 \cdot 945 = 30$.

The first few abundant numbers are 12, 18, 20, 24, 30, 36, 40, 42, 48, 54, 56, 60, 66, 70, $72, \ldots$ (sequence A005101 in the OEIS).

In fact, there are 21 abundant numbers less than 100 (12, 18, 20, 24, 30, 36, 40, 42, 48, 54, 56, 60, 66, 70, 72, 78, 80, 84, 88, 90, and 96), and all these numbers are even. As was noted above, the first odd abundant number is $945 = 3^3 \cdot 7 \cdot 5$.

It is easy to show that

- *any* $n = 2 \cdot 3^k$, $k > 1$, *is abundant.*

□ In fact,

$$\sigma(n) = 3 \cdot \frac{3^{k+1} - 1}{2} = 4,5 \cdot 3^k - 1,5 > 4 \cdot 3^k = 2n. \qquad \square$$

This allows us to state that there are infinitely many abundant numbers. Moreover, it is easy to show that

- *every multiple of a perfect number (except the perfect number itself) is abundant.*

For example, every multiple $n = 6m, m > 1$, of 6 greater than 6 is abundant because it has at least four proper divisors $1, \frac{n}{2}, \frac{n}{3}, \frac{n}{6}$, and for their sum, it holds that

$$1 + \frac{n}{2} + \frac{n}{3} + \frac{n}{6} = n + 1.$$

So, we get

$$\sigma(n) \geq 1 + \frac{n}{2} + \frac{n}{3} + \frac{n}{6} + n = 2n + 1 > 2n,$$

and n is abundant.

Similarly, it holds that

- *every multiple of an abundant number is abundant.*

For example, every multiple $n = 20m$ of 20 (including 20 itself) is abundant because it has at least five proper divisors, $\frac{n}{2}, \frac{n}{4}, \frac{n}{5}, \frac{n}{10}, \frac{n}{20}$, and for their sum, it holds that

$$\frac{n}{2} + \frac{n}{4} + \frac{n}{5} + \frac{n}{10} + \frac{n}{20} = n + \frac{n}{10}.$$

So, we get that

$$\sigma(n) \geq \frac{n}{2} + \frac{n}{4} + \frac{n}{5} + \frac{n}{10} + \frac{n}{20} + n = 2n + \frac{n}{10} > 2n,$$

and n is abundant.

□ In general, let $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, $k = p_1^{\beta_s} \cdot \ldots \cdot p_s^{\beta_s}$, where α_i and β_i are non-negative integers; let n be a perfect or an abundant number, i.e., $\sigma(n) \geq 2n$. Then, for $k > 1$, we have

$$\begin{aligned}\sigma(kn) &= \sigma(p_1^{\alpha_1+\beta_1} \cdot \ldots \cdot p_s^{\alpha_s+\beta_s}) = \frac{p_1^{\alpha_1+\beta_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+\beta_s+1} - 1}{p_s - 1}\\ &> \frac{p_1^{\alpha_1+\beta_1+1} - p_1^{\beta_1}}{p_1 - 1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+\beta_s+1} - p_s^{\beta_s}}{p_s - 1}\\ &= p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s} \cdot \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+1} - 1}{p_s - 1}\\ &= k\sigma(n) \geq 2kn,\end{aligned}$$

i.e., $\sigma(kn) > 2(kn)$, hence, the number kn is abundant. □

Consequently,

- *there are infinitely many abundant numbers; in particular, there are infinitely many even abundant numbers as well as infinitely many odd abundant numbers.*

□ It is east to see that, for example, any number of the form $12t$ is an even and any number of the form $945m$ is an odd abundant number. □

It was shown that the smallest abundant number is 12 and the smallest odd (i.e., not divisible by 2) abundant number is 945. It is easy to check that the smallest abundant number not divisible by 2 or by 3 is 5391411025 whose distinct prime factors are 5, 7, 11, 13, 17, 19, 23, and 29 (sequence A047802 in the OEIS).

An algorithm given by Iannucci in 2005 shows how to find the smallest abundant number not divisible by the first k primes:

- *If* $a(k)$ *is the smallest abundant number not divisible by the first* k *primes (for sufficiently large* k*), then for all* $\epsilon > 0$*, we have*

$$(1-\epsilon)\left(\frac{k}{\log k}\right)^{2-\epsilon} < \log a(k) < (1+\epsilon)\left(\frac{k}{\log k}\right)^{2+\epsilon}.$$

It is proven that

- *about* 24.74% *all positive integers are abundant.*

More exactly, a random positive integer is abundant or perfect with probability between 0.2474 and 0.2480. It means that the set of abundant and perfect numbers has a non-zero density, which is between 0.2474 and 0.2480 (Deléglise, 1998).

It is proven also that

- *every integer greater than* 20161 *can be written as the sum of two abundant numbers.*

Moreover, any even integer greater than 46 can be written as a sum of two abundant numbers; for more information, see the sequence A048242 in the OEIS.

3.5.4. An abundant number which is not the multiple of an abundant number or perfect number is called a *primitive abundant number*.

For example, 20 is a primitive abundant number because the sum of its proper divisors is $1 + 2 + 4 + 5 + 10 = 22 > 20$, but the sums of the proper divisors of 1, 2, 4, 5, and 10 are 0, 1, 3, 1, and 8, respectively; so, 20 is abundant, but each of its proper divisors is deficient, i.e., abundant number 20 is not a multiple of an abundant number or a perfect number.

The first such numbers are 20, 70, 88, 104, 272, 304, 368, 464, 550, 572, 650, 748, 836, 945, ... (sequence A071395 in the OEIS).

The smallest odd primitive abundant number is 945.

A variant definition of primitive abundant numbers is abundant numbers having no abundant proper divisor. They are: 12, 18, 20, 30, 42, 56, 66, 70, 78, 88, 102, 104, 114, 138, 174,... (sequence A091191 in the OEIS).

Of course, the sequence A071395 is a subsequence of A091191, as in the sequence A091191, not only all elements from A071395 (having only deficient proper divisors) numbers are represented but also all numbers which have perfect proper divisors. They are 12, 18, 30, 42, 56, 66, 78, 102, 114, 138, 174, 186, 196, 222, 246,... (sequence A275082 in the OEIS).

As any multiple of abundant or perfect number is abundant (see the previous item), it is obvious that

- *every multiple of a primitive abundant number is an abundant number.*

Moreover, it is easy to see that

- *every abundant number is a multiple of a primitive abundant number or a multiple of a perfect number.*

□ In fact, for a given abundant number n, if it has only deficient proper divisors, it is a primitive abundant, so it can be represented as its trivial multiple: $1 \cdot n$. If it has a perfect proper divisor m, it is a multiple of this perfect number: $n = mk$, $k > 1$. Finally, if it has an abundant divisor m, we get two possibilities. If m is a primitive abundant number, then we get the needed representation for n as a multiple of a primitive abundant number: $n = mk$. $k > 1$. If abundant number m is not primitive abundant, then we repeat our consideration for a new abundant number m, $m < n$. Now, we get the fool-proof proposition after finite number of steps. □

It is possible to show that

- *there are an infinite number of primitive abundant numbers.*

Moreover, it is proven (Erdős, 1934) that

- *the number of primitive abundant numbers less than or equal to* n *is* $o(\frac{n}{\log^2 n})$.

Moreover, it is shown that *every primitive abundant number is either a primitive semiperfect number or a weird number.* We talk about these classes of numbers in Chapter 5.

3.5.5. A *highly abundant number* is a positive integer n for which the sum of its positive integer divisors is greater than the sum of the positive integer divisors of any smaller positive integer number:

$$\sigma(n) > \sigma(m) \quad \text{for} \quad n > m, \ n, m \in \mathbb{N}.$$

For example, 8 is highly abundant because $\sigma(8) = 8 + 4 + 2 + 1 = 15$ is larger than all previous values of σ: $\sigma(7) = 8$, $\sigma(6) = 12$, $\sigma(5) = 6$, $\sigma(4) = 7$, $\sigma(3) = 4$, $\sigma(2) = 3$, $\sigma(1) = 1$.

On the other hand, 5 is not highly abundant because $\sigma(5) = 5 + 1 = 6$ is smaller than $\sigma(4) = 4 + 2 + 1 = 7$.

The first few highly abundant numbers are 1, 2, 3, 4, 6, 8, 10, 12, 16, 18, 20, 24, 30, 36, 42, ... (sequence A002093 in the OEIS).

Highly abundant numbers were first introduced by Pillai (1943), and an early work on the subject was done by Alaoglu and Erdős (1944), who tabulated all such numbers up to 10^4.

Despite the terminology, not all highly abundant numbers are abundant numbers. In particular, none of the first seven highly abundant numbers 1, 2, 3, 4, 6, 8, and 10 is abundant. However, with 16, the ninth highly abundant number,

- *eight numbers,* $1, 2, 3, 4, 6, 8, 10, 16$, *are the only highly abundant numbers that are not abundant.*

It can be proved that

- *the only odd highly abundant numbers are* 1 *and* 3.

For example, 5 is not highly abundant because $\sigma(5) = 5+1 = 6$ is smaller than $\sigma(4) = 7$. The number 7 is not highly abundant because $\sigma(7) = 7 + 1 = 8$ is smaller than $\sigma(6) = 12$. The number 9 is not highly abundant because $\sigma(9) = 13$ is smaller than $\sigma(8) = 15$.

It is easy to check that the first eight factorials $n!$, $n = 1, 2, 3, 4, 5, 6, 7, 8$, are highly abundant. However, *not all factorials are highly abundant.* For example,

$$\sigma(9!) = \sigma(362880) = 1481040,$$

but there is a smaller number with larger sum of divisors,

$$\sigma(360360) = 1572480,$$

so 9! is not highly abundant.

A positive integer n is called a *powerful number* (or *square-full number* or *2-powerful number*) if for every prime number p dividing n, p^2 also divides n. The sequence of these numbers starts from 1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 72, 81, 100, 108, ... (sequence A001694 in the OEIS). It is easy to see that we can find some highly abundant numbers which are powerful: They start from 1, 4, 8, 16, 36, ... However, it is proven by Nicolas (1969), that 7200 is the largest powerful number that is also highly abundant. All larger highly abundant numbers have a prime factor that divides them only once. Therefore, 7200 is also the largest highly abundant number with an odd sum of divisors.

Alaoglu and Erdős (1044) tabulated all highly abundant numbers up to 10^4 and showed that

- *the number of highly abundant numbers less than x is at least proportional to* $\log^2 x$.

They noted also that all superabundant numbers (see the next item) are highly abundant and asked whether there are infinitely many highly abundant numbers that are not superabundant. This question was answered affirmatively by Nicolas (1969).

3.5.6. A *superabundant number* is a positive integer n such that for all positive integers $m < n$, it holds that

$$\frac{\sigma(m)}{m} < \frac{\sigma(n)}{n}.$$

For example, the number 6 (with $\sigma(6) = 12$) is a superabundant number because for the numbers $m = 1, 2, 3, 4$, and 5, the sigma function $\sigma(m) = 1, 3, 4, 7$, and 6, and

$$\frac{12}{6} > \frac{1}{1}, \frac{12}{6} > \frac{3}{2}, \frac{12}{6} > \frac{4}{3}, \frac{12}{6} > \frac{7}{4}, \frac{12}{6} > \frac{6}{5}.$$

On the other hand, the number 5 (with $\sigma(5) = 6$) is not a superabundant number because for $m = 4$, the sigma function $\sigma(m) = 7$, and $\frac{7}{4} > \frac{6}{5}$.

The first few superabundant numbers are 1, 2, 4, 6, 12, 24, 36, 48, 60, 120, 180, 240, 360, 720, 840,... (sequence A004394 in the OEIS).

Superabundant numbers were defined by Leonidas Alaoglu and Paul Erdős (1944). In particular, they proved that *if n is superabundant, the prime decomposition of n has non-increasing exponents and that all primes up to p_k are factors of n*:

- *If n is a superabundant number, then there exist $k \in \mathbb{N}$ and $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$ such that*

  $$n = 2^{\alpha_2} 3^{\alpha_3} \ldots p_k^{\alpha_k},$$

  where p_i is the ith prime number, and $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_k \geq 1$.

□ In fact, if there exist two primes $p = p_i, q = p_j$ such that $p_i < p_j$ and $\alpha = \alpha_i < \alpha_j = \beta$, then the number $m = \frac{np}{q} < n$, and hence, $\frac{\sigma(m)}{m} < \frac{\sigma(n)}{n}$. This inequality reduces to

$$\frac{p^{\alpha+1} - 1}{p^{\alpha+1} - p} < \frac{q^{\beta+1} - 1}{q^{\beta+1} - q}.$$

As $\frac{x^n - 1}{x^n - x}$ is a decreasing function of x and n for $x, n \geq 2$, a simple calculation shows that our inequality is not satisfied.

Similar arguments can be used when we are going to show that the k given prime numbers p_i must be precisely the first k prime numbers 2, 3, 5, ...; if not, we could replace one of the given primes by a smaller prime and thus obtain a smaller number than m, which again gives a contradiction to the inequality $\frac{\sigma(m)}{m} < \frac{\sigma(n)}{n}$. □

As a simple corollary of this property, it holds that

- *all superabundant numbers greater than* 1 *are even positive integers.*

Also, it was proven by Leonidas Alaoglu and Paul Erdős (1944) that

- *except in two special cases,* $n = 4$ *and* $n = 36$*, the last exponent* α_k *must equal* 1.

It means that

- *the numbers* $1, 4,$ *and* 36 *are the only square superabundant numbers.*

As a superabundant number, n has the form $n = 2^{\alpha_2}3^{\alpha_3}\dots p_k^{\alpha_k}$, where p_i is the ith prime number, then in particular

- *any superabundant number is a multiple of the* k*th primorial* $p_k\#$.

Moreover, saying that the sequence $\alpha_1, \alpha_2, \dots, \alpha_k$ of exponents is non-increasing (i.e., $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_k \geq 1$) is equivalent to saying that

- *a highly composite number is a product of primorials.*

Alaoglu and Erdős observed also that

- *any superabundant number is a highly abundant number.*

□ In fact, if n is superabundant, then, by definition, for any $m < n$, it holds that $\frac{\sigma(m)}{m} < \frac{\sigma(n)}{n}$, and we have

$$n\sigma(m) < m\sigma(n) < n\sigma(n), \text{ or } \sigma(m) < \sigma(n).$$

Therefore, for any $m < n$, it holds that $\sigma(m) < \sigma(m)$, and by definition, n is highly abundant. □

However (see the next item for definitions),

- *not all superabundant numbers are colossally abundant.*

Moreover, superabundant numbers are closely related to *highly composite numbers* (see the next section for definitions). However, not all superabundant numbers are highly composite numbers as well as not all highly composite numbers are superabundant. For instance, 7560 is highly composite but not superabundant. Conversely, 1163962800 is superabundant but not highly composite.

In fact, only 449 superabundant and highly composite numbers are the same; the first few of them are 1, 2, 4, 6, 12, 24, 36, 48, 60, 120, 180, 240, 360, 720, 840, …, while the last few has the form $2^{10} \cdot 3^6 \cdot 5^4 \cdot 7^3 \cdot 11^3 \cdot 13^2 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29 \cdot 31 \cdot 37 \cdot \ldots \cdot 347$ (sequence A166981 in the OEIS).

3.5.7. Superabundant numbers are also of interest in connection with the *Riemann hypothesis.* In fact, in 1915, Ramanujan proved that under the assumption of the Riemann hypothesis, the inequality

$$\sigma(n) < e^{\gamma} n \log\log n$$

(the so-called *Robin's inequality*), where $\gamma = 0.5772156649\ldots$ if the Euler–Mascheroni constant holds for all sufficiently large n.

This inequality is known to fail for 27 numbers (sequence A067698 in the OEIS): 2, 3, 4, 5, 6, 8, 9, 10, 12, 16, 18, 20, 24, 30, 36, 48, 60, 72, 84, 120, 180, 240, 360, 720, 840, 2520, and 5040.

The largest known value that violates the inequality is 5040, a superabundant number.

In 1984, Guy Robin proved that the inequality is true for all $n > 5040$ if and only if the Riemann hypothesis is true.

This is *Robin's theorem* and the inequality became known after him.

Robin furthermore showed that if the Riemann hypothesis is false, then there are an infinite number of values of n that violate the inequality; and it is known that the smallest such $n > 5040$ must be superabundant (Akbary and Friggstad, 2009).

3.5.8. A *generalized k-super abundant number*, $k \in \mathbb{N}$, is a number n such that for all $m < n$ it holds that

$$\frac{\sigma_k(m)}{m^k} < \frac{\sigma_k(n)}{n^k},$$

where $\sigma_k(n) = \sum_{d|n} d^k$ is the sum of the kth powers of the positive integer divisors of n.

For example, 4 is a 2-super abundant number since $\sigma_2(4) = 1^2 + 2^2 + 4^2 = 22$, and for numbers $m = 1, 2$, and 3 the values of $\sigma_2(m)$

are 1, 5, and 10; therefore,

$$\frac{22}{16} > \frac{1}{1}, \; \frac{22}{16} > \frac{5}{4}, \text{ and } \frac{22}{16} > \frac{10}{9}.$$

The first generalized 2-super abundant numbers are 1, 2, 4, 6, 12, 24, 48, 60, 120, 240, 360, 720, 840, 1680, 2520, ... (sequence A208767 in the OEIS).

It is easy to see that 1-super abundant numbers are just superabundant numbers, while 0-super abundant numbers are highly composite numbers (see the next section for definitions).

3.5.9. A *colossally abundant number* is a positive integer n, for which there exists an $\epsilon > 0$ such that for all $k > 1$, it holds that

$$\frac{\sigma(n)}{n^{1+\epsilon}} \geq \frac{\sigma(k)}{k^{1+\epsilon}}.$$

The first few colossally abundant numbers are 2, 6, 12, 60, 120, 360, 2520, 5040, 55440, 720720, 1441440, 4324320, 21621600, 367567200, 6983776800, ... (sequence A004490 in the OEIS). In fact, there are exactly 22 of them less than 10^{18}.

It is easy to show that

- *all colossally abundant numbers are also superabundant numbers.*

□ In fact, if n is a colossally abundant number, then for any $m < n$, it holds that $\frac{\sigma(n)}{n^{1+\epsilon}} \geq \frac{\sigma(m)}{m^{1+\epsilon}}$; then, we get

$$m^{\epsilon} \cdot \frac{\sigma(n)}{n} > n^{\epsilon} \cdot \frac{\sigma(m)}{m} > m^{\epsilon} \cdot \frac{\sigma(m)}{m},$$

or $\frac{\sigma(n)}{n} > \frac{\sigma(m)}{m}$. So, for any $m < n$, it holds that $\frac{\sigma(m)}{m} < \frac{\sigma(n)}{n}$, and by definition, n is superabundant. □

However, the converse is not true. The first few superabundant numbers, which are not colossally abundant, are 1, 4, 24, 36, 48, 180, 240, 720, 840, 1260, ...

One can check that the first 15 colossally abundant numbers are also the first 15 *superior highly composite numbers* (see the next section for definitions), but neither set is a subset of the other. For example, the number 160626866400 is colossally abundant but not superior highly composite, while 13967553600 is superior highly composite but not colossally abundant.

Colossally abundant numbers were first studied by Ramanujan and were later reconsidered in a slightly stronger form in a 1944 paper by Leonidas Alaoglu and Paul Erdős in which they tried to extend Ramanujan's results.

Just like with superabundant numbers, an effective construction of the set of all colossally abundant numbers is given by the following monotonic mapping from the positive real numbers:

- *If for a given real* $\epsilon > 0$ *and for any prime number* p*, the value* $\alpha_p(\epsilon)$ *is defined as*

  $$\alpha_p(\epsilon) = \left\lfloor \frac{\log\left(1 + \frac{p-1}{p^{1+\epsilon}-p}\right)}{\log p} \right\rfloor,$$

  then

  $$n(\epsilon) = \prod_{p \in P} p^{\alpha_p(\epsilon)}$$

  is a colossally abundant number.

So, colossally abundant numbers capture the notion of having many divisors by requiring them to maximize, for some $\epsilon > 0$, the value of the function $\frac{\sigma(n)}{n^{1+\epsilon}}$ over all values of n. The classical number-theoretical results (see Chapter 2) ensures that for every $\epsilon > 0$, this function has a maximum and that as $\epsilon \to 0$, these maxima will increase. Thus, there are infinitely many colossally abundant numbers, although they are rather sparse.

In spite of the fact that for every ϵ, the function $\frac{\sigma(n)}{n^{1+\epsilon}}$ has a maximum, it is not obvious and, in fact, not true that for every ϵ this maximum value is unique.

Alaoglu and Erdős studied how many different values of n could give the same maximal value of the above function for a given value of ϵ.

They showed that for most values of ϵ there would be a single integer n maximizing the function.

Later, however, Erdős and Jean-Louis Nicolas showed that for a certain set of discrete values of ϵ there could be two or four different values of n giving the same maximal value.

Alaoglu and Erdős conjectured that

- *the ratio of two consecutive colossally abundant numbers was always a prime number.*

Alaoglu and Erdős's conjecture remains open, although it has been checked up to at least 10^7. If it is true, one can state that

- *there exists a sequence of non-distinct prime numbers* $p_1, p_2, p_3, \ldots$ *such that the nth colossally abundant number is of the form* $\prod_{i=1}^{n} p_i$.

Assuming the conjecture holds, this sequence of primes starts from 2, 3, 2, 5, 2, 3, 7, 2, 11, 13, 2, 3, 5, 17, 19, ... (sequence A073751 in the OEIS).

As was noted above, if the Riemann hypothesis is false, a colossally abundant number will be a counterexample.

Perfect numbers and highly composite numbers

In this section, we consider some classes of special numbers, closely connected with perfect numbers but defined using number of divisors function $\tau(n) = \sum_{d|n} 1$.

3.5.10. A *highly composite number* (or *anti-prime number*) is a positive integer n with more divisors than any smaller positive integer m has; for any $m < n$, it holds that

$$\tau(m) < \tau(n).$$

For example, the number 4 is highly composite, as $\tau(4) = 3$, while $\tau(3) = 2$, $\tau(2) = 2$, and $\tau(1) = 1$. On the other hand, the number 5 is not highly composite, as $\tau(5) = 2$, while $\tau(4) = 3$.

The first few highly composite numbers are 1, 2, 4, 6, 12, 24, 36, 48, 60, 120, 180, 240, 360, 720, 840, ... (sequence A002182 in the

OEIS). The corresponding number of divisors is 1, 2, 3, 4, 6, 8, 9, 10, 12, 16, 18, 20, 24, 30, 32, . . . (sequence A002182 in the OEIS).

Note that a related concept of largely composite number refers to a positive integer which has at least as many divisors as any smaller positive integer.

The name can be somewhat misleading as two highly composite numbers (1 and 2) are not actually composite numbers. However, it is obvious that

- *any highly composite number greater than* 2 *is composite.*

□ In fact, if p is an odd prime number, then $\tau(p) = 2$, while $\tau(p-1) \geq 3$. □

There exists an explicit formula:

- *A highly composite number has the form*

$$n = 2^{\alpha_2}3^{\alpha_3}\dots p_k^{\alpha_k},$$

where the k given prime numbers p_i must be precisely the first k prime numbers $2, 3, 5, \dots$, *and* $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_k$.

□ In fact, for the construction of a highly composite number, we should use the first primes; if not, we could replace one of the given primes by a smaller prime and thus obtain a smaller number than n with the same number of divisors (for instance, $10 = 2 \cdot 5$ may be replaced with $6 = 2 \cdot 3$; both have four divisors).

The sequence of exponents must be non-increasing, that is $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_k$; otherwise, by exchanging two exponents, we would again get a smaller number than n with the same number of divisors (for instance, $18 = 2^1 \cdot 3^2$ may be replaced with $12 = 2^2 \cdot 3^1$; both have six divisors). □

Roughly, for a number to be a highly composite, it has to have prime factors as small as possible but not too many of the same.

Also, *except in two special cases* $n = 4$ *and* $n = 36$, *the last exponent* α_k *must equal* 1. It means that

- *the numbers* $1, 4$, *and* 36 *are the only square highly composite numbers.*

Saying that the sequence of exponents is non-increasing is equivalent to saying that

- *a highly composite number is a product of primorials.*

Although the above-described conditions are necessary, they are not sufficient for a number to be highly composite. For example, $96 = 2^5 \cdot 3$ satisfies the above conditions and has 12 divisors but is not highly composite since there is a smaller number 60 which has the same number of divisors.

It is easy to check that

- *there are infinitely many highly composite numbers.*

☐ In fact, if n is highly composite, then $2n$ has more divisors than n: $2n|2n$ as well as any divisor of n. So, between n and $2n$, there should be a highly composite number. ☐

It is possible that Plato must have known about highly composite numbers, as he deliberately chose the number 5040, which has more divisors than any numbers less than it, as the ideal number of citizens in a city. Ramanujan [Rama15] listed 102 highly composite numbers up to 6746328388800 but omitted 293318625600. Robin (1983) gives the first 5000 highly composite numbers, and a comprehensive survey is given by Nicholas (1988). Flammenkamp gives a list of the first 779674 highly composite numbers.

Moreover, it is possible to prove that

- *all highly composite numbers greater than 6 are also abundant numbers.*

☐ One need only look at the three largest proper divisors of a particular highly composite number to ascertain this fact. ☐

One can check also that 10 of the first 38 highly composite numbers are superior highly composite numbers (see the last item for definitions).

3.5.11. A *superior highly composite number* is a positive integer number n which has more divisors per some positive power of itself than any other number: There exists an $\epsilon > 0$ such that for all $k > 1$, it holds that

$$\frac{\tau(n)}{n^\epsilon} \geq \frac{\tau(k)}{k^\epsilon}.$$

The term was coined by Ramanujan [Rama15].

The first superior highly composite numbers are 2, 6, 12, 60, 120, 360, 2520, 5040, 55440, 720720, 1441440, 4324320, 21621600, 367567200, 6983776800 (sequence A002201 in the OEIS).

The condition for a superior highly composite number is a stronger restriction than that of a highly composite number, which is defined as having more divisors than any smaller positive integer. In fact,

- *any superior highly composite number is highly composite.*

□ In fact, let n be superior highly composite but not highly composite. Then, there is some number $m < n$ such that $\tau(n) \leq \tau(m)$. Then,

$$\frac{\tau(m)}{m^\epsilon} \geq \frac{\tau(n)}{m^\epsilon} > \frac{\tau(n)}{n^\epsilon}$$

for all $\epsilon > 0$, so a number n cannot be superior highly composite. □

Moreover, the first 15 superior highly composite numbers, 2, 6, 12, 60, 120, 360, 2520, 5040, 55440, 720720, 1441440, 4324320, 21621600, 367567200, and 6983776800, are also the first 15 colossally abundant numbers, which meet a similar condition based on the sum of divisors function rather than the number of divisors. Neither set, however, is a subset of the other. For example, the number 13967553600 is superior highly composite but not colossally abundant, while 160626866400 is colossally abundant but not superior highly composite.

An effective construction of the set of all superior highly composite numbers is given by the following monotonic mapping:

- *Let for a given real* $\epsilon > 0$ *and for any prime number* p *the value* $\alpha_p(\epsilon)$ *be defined as*

$$\alpha_p(\epsilon) = \left\lfloor \frac{1}{p^\epsilon - 1} \right\rfloor;$$

then, the number

$$n(\epsilon) = \prod_{p \in P} p^{\alpha_p(\epsilon)}$$

is a superior highly composite number.

The product to calculate $n(\epsilon)$ should be terminated for $p \geq 2^{\epsilon}$ because if $p > 2^x$, then $\alpha_p(\epsilon) = 0$.

Moreover, for each superior highly composite number m, there exists a half-open interval $I \subset \mathbb{R}^+$ such that for any $x \in I$, it holds that $n(\frac{1}{x}) = m$. This representation implies that *the quotient of two successive superior highly composite numbers is a prime number*. In other words,

- *there exists an infinite sequence* $p_1, p_2, p_3, \ldots, p_k \ldots$ *of prime numbers such that the nth superior highly composite number has the form* $p_1 p_2 \ldots p_n$.

The first such prime numbers are 2, 3, 2, 5, 2, 3, 7, 2, 11, 13, 2, 3, 5, 17, 19, … (sequence A000705 in the OEIS).

Perfect numbers and practical numbers

3.5.12. A *practical number* (or *panarithmic number*) is a positive integer n such that all smaller positive integers can be represented as sums of distinct divisors of n.

For example, 12 is a practical number because all the numbers from 1 to 11 can be expressed as sums of its divisors 1, 2, 3, 4, and 6, as well as these divisors themselves:

$$5 = 3 + 2,\ 7 = 6 + 1,\ 8 = 6 + 2,$$

$$9 = 6 + 3,\ 10 = 6 + 3 + 1,\ 11 = 6 + 3 + 2.$$

The sequence of practical numbers begins as follows: 1, 2, 4, 6, 8, 12, 16, 18, 20, 24, 28, 30, 32, 36, 40, … (sequence A005153 in the OEIS).

3.5.13. Practical numbers were used by Fibonacci in his *Liber Abaci* (1202) in connection with the problem of representing rational numbers as Egyptian fractions. The name "practical number" is due to

Srinivasan (1948). He was the first to attempt a classification of these numbers. His partial characterization was extended and completed by Stewart (1954) and Sierpiński (1955).

This characterization makes it possible to determinate whether a number is practical by examining its prime factorization:

- *A positive integer* $n > 1$ *with prime factorization* $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, *where* $p_1 < p_2 < \cdots < p_k$, *is practical if and only if each of its prime factors* p_i *is small enough for* $p_i - 1$ *to have a representation as a sum of smaller divisors; for this to be true, the first prime* p_1 *must equal* 2, *and for every* i *from* 2 *to* k, *each successive prime* p_i *must obey the inequality*

$$p_i \leq 1 + \sigma(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{i-1}^{\alpha_{i-1}}) = 1 + \prod_{j=1}^{i-1} \frac{p_j^{\alpha_j+1} - 1}{p_j - 1}.$$

For example, $2 \cdot 3^2 \cdot 29 \cdot 823 = 429606$ is practical because the inequality above holds for each of its prime factors: The first prime factor is 2, $3 \leq \sigma(2) + 1 = 4$, $29 \leq \sigma(2 \cdot 3^2) + 1 = 40$, and $823 \leq \sigma(2 \cdot 3^2 \cdot 29) + 1 = 1171$.

□ The condition stated above is necessary and sufficient for a number to be practical.

In one direction, this condition is necessary in order to be able to represent $p_i - 1$ as a sum of divisors of n because if the inequality failed to be true, then even adding together all the smaller divisors would give a sum too small to reach $p_i - 1$.

In the other direction, the condition is sufficient, as can be shown by induction.

More strongly, we can prove that if the factorization of n satisfies the condition above, then any $m \leq \sigma(n)$ can be represented as a sum of divisors of n by the following sequence of steps:

I. By induction on $j \in [1, \alpha_k]$, it can be shown that

$$p_k^j \leq 1 + \sigma\left(\frac{n}{p_k^{\alpha_k-(j-1)}}\right).$$

Therefore, it holds that $p_k^{\alpha_k} \leq 1 + \sigma(n/p_k)$.

II. Since, due to **I**, the internals $[qp_k^{\alpha_k}, qp_k^{\alpha_k} + \sigma(n/p_k)]$ cover $[1, \sigma(n)]$ for $0 \leq q \leq \sigma(n/p_k^{\alpha_k})$, there are such a q and some $r \in [0, \sigma(n/p_k)]$ for which $m = qp_k^{\alpha_k} + r$.

III. Since $q \leq \sigma\big(\frac{n}{p_k^{\alpha_k}}\big)$ and $\frac{n}{p_k^{\alpha_k}}$ can be shown by induction to be practical, we can find a representation of q as a sum of divisors of $\frac{n}{p_k^{\alpha_k}}$.

IV. Since $r \leq \sigma(\frac{n}{p_k})$ and since $\frac{n}{p_k}$ can be shown by induction to be practical, we can find a representation of r as a sum of divisors of $\frac{n}{p_k}$.

V. The divisors representing r, together with $p_k^{\alpha_k}$ times each of the divisors representing q, together form a representation of m as a sum of divisors of n. □

3.5.14. Now, it is easy to show that

- *every even perfect number is also a practical number.*

□ This follows from Leonhard Euler's result that an even perfect number must have the form $2^{p-1}(2^p - 1)$, where $2^p - 1 \in P$. The odd part of this factorization is equal to the sum of the divisors of the even part, so every odd prime factor of such a number must be at most the sum of the divisors of the even part of the number. Therefore, this number must satisfy the characterization of practical numbers. Formally, the prime representation of an even perfect number has the following property: The first prime is 2 and the second prime $2^p - 1 \leq 1 + \sigma(2^{p-1}) = 1 + (2^p - 1) = 2^p$. □

Moreover,

- *every power of two is a practical number.*

□ Obviously, powers of two 2^α, $\alpha \in \mathbb{N}$, satisfy the characterization of practical numbers in terms of their prime factorizations: The only prime in their factorizations, p_1, equals two as required. However, there exists a much simpler explanation: Any binary representation of a given positive integer $n \leq 2^\alpha$ is a representation of this number as a sum of distinct divisors $1, 2, 2^2, \ldots, 2^\alpha$ of the number 2^α. □

The practical numbers have many interesting properties. It is easy to show that

- *the only odd practical number is* 1.

□ In fact, if n is an odd number greater than 2, then 2 cannot be expressed as the sum of distinct divisors of n. □

More strongly, Srinivasan (1948) observes that

- *other than* 1 *and* 2*, every practical number is divisible by* 4 *or* 6.

Due to properties of divisor function, it is obvious that

- *the product of two practical numbers is also a practical number.*

So, we can state that

- *the set of all practical numbers is closed under multiplication.*

Moreover, it holds that

- *the least common multiple of any two practical numbers is also a practical number.*

From the above characterization by Stewart and Sierpiński, it can be seen that

- *if n is a practical number and d is one of its divisors, then $n \cdot d$ must also be a practical number.*

□ It follows form the properties of divisors of the number $n \cdot d$. For example, as 6 is practical, we get that any number $2 \cdot 3^{\alpha}$, $\alpha \in \mathbb{N}$, must be a practical number as well as any number $3 \cdot 2^{\alpha}$, $\alpha \in \mathbb{N}$. □

The above property allow us to consider the set of *primitive practical numbers*: those having no proper practical divisors.

The sequence of primitive practical numbers starts from the numbers 1, 2, 6, 20, 28, 30, 42, 66, 78, 88, 104, 140, 204, 210, 220, … (sequence A267124 in the OEIS).

Using the property above, it is easy to prove that

- *any primitive practical number is either square-free, or when divided by any of its prime factors whose factorization exponent is greater than* 1 *is no longer practical.*

It is easy to check that

- *every primorial is practical.*

□ For the first two primorials, 2 and $2 \cdot 3 = 6$, this is clear. Each successive primorial is formed by multiplying a prime number p_i by a smaller primorial that is divisible by both 2 and the next smaller prime, p_{i-1}. By Bertrand's postulate, $p_i < 2p_{i-1}$, so each successive prime factor in the primorial is less than one of the divisors of the previous primorial. By induction, it follows that every primorial satisfies the characterization of practical numbers. Because a primorial is, by definition, square-free, it is also a primitive practical number. □

Generalizing the primorials, we get that

- *any number that is the product of non-zero powers of the first k primes must also be practical.*

□ It is obvious, as any such number can be obtained from the corresponding primorial by repeated multiplication by some of its divisors. This includes Ramanujan's highly composite numbers as well as the factorial numbers $n!$ □

So, we obtained two more classes of practical numbers:

- *Any highly composite number as well as any factorial number is practical.*

3.5.15. One reason for interest in practical numbers is that many of their properties are similar to properties of the prime numbers.

Indeed, theorems analogous to Goldbach's conjecture and the twin prime conjecture are known for practical numbers:

- *Every positive even integer is the sum of two practical numbers, and there exist infinitely many triples of practical numbers* $(x-2, x, x+2)$.

Melfi also showed that

- *there are infinitely many practical Fibonacci numbers.*

The analogous question of the existence of infinitely many Fibonacci primes is open.

Hausman and Shapiro (1984) showed that

- *there always exists a practical number in the interval* $[x^2, (x+1)^2)]$ *for any positive real* x.

This result is analogous to Legendre's conjecture for primes.

Perfect numbers and Ore numbers

3.5.16. An *Ore number* (or *harmonic divisor number* or *Ore harmonic number*) is a positive integer whose divisors have a *harmonic mean* that is an integer.

Recall that the *harmonic mean* can be expressed as the reciprocal of the arithmetic mean of the reciprocals of the given set of observations.

As a simple example, the harmonic mean of the four divisors 1, 2, 3, and 6 of 6 is an integer:

$$\frac{4}{\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{6}} = \frac{\tau(6)}{\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{6}} = 2.$$

The first Ore numbers are 1, 6, 28, 140, 270, 496, 672, 1638, 2970, 6200, 8128, 8190, … (sequence A001599 in the OEIS).

In fact, the reciprocals of the divisors of any perfect number n must add up to 2. To get this, take the definition of a perfect number, $\sigma(n) = 2n$, and divide both sides by n.

So, for 6 and 28, we have

$$\frac{1}{6}+\frac{1}{3}+\frac{1}{2}+\frac{1}{1} = 2;\ \ \frac{1}{28}+\frac{1}{14}+\frac{1}{7}+\frac{1}{4}+\frac{1}{2}+\frac{1}{1} = 2.$$

Moreover, the number of divisors of a perfect number, n, (whether even or odd) must be even because n cannot be a perfect square.

From these two results, proved in Section 3.3, it follows that

- *every perfect number is an Ore number.*

Ore conjectured that *no odd harmonic divisor numbers exist other than 1.* If the conjecture is true, this would imply the non-existence of odd perfect numbers.

Perfect numbers and Mersenne numbers

3.5.17. In this section, we discuss main connections between perfect numbers and other classes of special numbers. We considered already such connections, generated by divisor functions $\sigma(n)$, $s(n)$, and $\tau(n)$. This approach is based on the definition of perfect numbers as well as deficient numbers, abundant numbers, and their relatives.

The next natural approach should be based on the formula $2^{p-1}(2^p-1)$, which generates all even perfect numbers using prime numbers of the form 2^p-1, i.e., *Mersenne primes* $M_p = 2^p - 1$.

Recall that a *Mersenne number* is a positive integer of the form

$$M_n = 2^n - 1, \ n \in \mathbb{N}.$$

The first Mersenne numbers are 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, 16383, 32767, ... (sequence A000225 in OEIS).

For $2^n - 1$ to be prime, it is necessary that n itself be prime. Mersenne numbers $2^p - 1$ with prime p form the sequence 3, 7, 31, 127, 2047, 8191, 131071, 524287, 8388607, 536870911, ... (sequence A001348 in OEIS).

In fact, the exponents n which give Mersenne primes are 2, 3, 5, 7, 13, 17, 19, 31, ... (sequence A000043 in the OEIS), and the resulting Mersenne primes are 3, 7, 31, 127, 8191, 131071, 524287, 2147483647, ... (sequence A000668 in the OEIS).

In this chapter (as well as in Chapter 2), we considered and used a lot of important facts about Mersenne numbers. In this section, some minor additional problems are represented.

3.5.18. A *double Mersenne number* is a Mersenne number of the form

$$M_{M_n} = 2^{2^n-1} - 1, \ n \in \mathbb{N}.$$

The first few double Mersenne numbers are $M_{M_1} = 1$, $M_{M_2} = M_3 = 7$, $M_{M_3} = M_7 = 127$, $M_{M_4} = M_{15} = 32767$ (sequence A077586 in the OEIS).

A double Mersenne number that is prime is called a *double Mersenne prime.*

Since a Mersenne number M_n can be prime only if n is prime, a double Mersenne number M_{M_p} can be prime only if M_p is prime.

The first values of p for which M_p is a prime are $p = 2, 3, 5, 7, 13, 17, 19, 31$. Of these, M_{M_p} is known to be prime for $p = 2$, $3, 5, 7$; for $p = 13$, $17, 19$, and 31, M_{M_p} is composite, and its explicit factors have been found.

If another double Mersenne prime will be ever be found, it would almost certainly be the largest known prime number.

Using the sequence of double Mersenne primes, we can consider the notion of *double perfect number*, i.e., an even perfect number of the form $2^{M_p-1}(2^{M_p} - 1)$, where $M_p = 2^p - 1$ and $M_{M_p} = 2^{M_p} - 1$ are both Mersenne primes. For $p = 2$, we get $M_p = 3$, $M_{M_p} = 7$, and hence, the number $2^{M_p-1}(2^{M_p} - 1) = 28$; For $p = 3$, we get $M_p = 7$, $M_{M_p} = 127$, and hence, the number $2^{M_p-1}(2^{M_p} - 1) = 8128$. For $p = 5$, we get $M_p = 31$, $M_{M_p} = 2147483647$, and hence, the number $2^{M_p-1}(2^{M_p} - 1) = 2^{30} \cdot (2^{31} - 1) = 230584\ldots952128$ (19 digits).

Are there more double perfect numbers? Is the set of such numbers infinite? It is interesting to study the behavior and properties of this subset of even perfect numbers.

3.5.19. There exists another interesting subsequence of Mersenne numbers.

A *Woodall number* W_n is a positive integer of the form

$$W_n = n \cdot 2^n - 1, \; n \in \mathbb{N}.$$

The first few Woodall numbers are 1, 7, 23, 63, 159, 383, 895, 2047, 4607, 10239, … (sequence A003261 in the OEIS).

It is easy to check that for a positive integer m,

- *the Woodall number* W_{2^m} *may be prime only if* $2^m + m$ *is prime.*

It means that a Woodall prime W_{2^m} should coincide with a Mersenne prime M_{2^m+m}. As of 2020, the only known primes that are both Woodall primes and Mersenne primes are $W_2 = M_3 = 7$ and $W_{512} = M_{521}$.

So, we state that the only known even perfect numbers, which are generated by a Woodall primes, are $28 = 2^2 W_2$ and $2^{520} W_{512}$.

3.5.20. A *Carol number* is an integer of the form

$$CN(n) = 4^n - 2^{n+1} - 1,\ n \in \mathbb{N}.$$

An equivalent formula is

$$CN(n) = (2^n - 1)^2 - 2,\ n \in \mathbb{N}.$$

The first few Carol numbers are -1, 7, 47, 223, 959, 3967, 16127, 65023, 261119, 1046527, … (sequence A093112 in OEIS).

These numbers were first encountered by C. Emmanuel in 1994, who consequently named them after a friend, Carol G. Kirnon.

For $n > 2$, the binary representation of the nth Carol number is $n-2$ consecutive unities, a single zero in the middle, and $n+1$ more consecutive unities or, to put it algebraically,

$$CN(n) = \sum_{i=1, i \neq n+2}^{2n} 2^{i-1}.$$

So, for example, 47 is 101111 in binary, while 223 is 11011111 in binary, etc.

The difference between the nth Mersenne number and the nth Carol number is 2^{n+1}:

$$M_n - CN(n) = 2^{n+1} = M_{n+1} + 1.$$

So, for prime p it holds that $M_p = CN(p) + 2^{p+1}$, and if M_p is prime too, we get a representation of the corresponding even perfect number $2^{p-1} M_p$ in the form

$$2^{p-1}(CN(p) + 2^{p+1}) = 2^{p-1} CN(p) + 4^p.$$

3.5.21. A *Kynéa number* is an positive integer of the form

$$KN(n) = 4^n + 2^{n+1} - 1,\ n \in \mathbb{N}.$$

An equivalent formula is

$$KN(n) = (2^n + 1)^2 - 2,\ n \in \mathbb{N}.$$

The first few Kynèa numbers are 7, 23, 79, 287, 1087, 4223, 16639, 66047, 263167, 1050623, … (sequence A093069 in the OEIS).

The binary representation of the nth Kynèa number is a single leading unity, followed by $n-1$ consecutive zeros, followed by $n+1$ consecutive unities or, to put it algebraically,

$$KN(n) = 2^{2n} + \sum_{i=0}^{n} 2^i.$$

So, for example, 23 is 10111 in binary, 79 is 1001111 in binary, etc.

It is easy to see that the Kynèa number is the nth power of 4 plus the $(n+1)$th Mersenne number:

$$KN(n) = 4^n + M_{n+1}.$$

So, for prime p, it holds that $M_p = KN(p-1) - 4^{p-1}$, and if M_p is prime too, we get a representation of the corresponding even perfect number $2^{p-1}M_p$ in the form

$$2^{p-1}(KN(p-1) - 4^{p-1}) = 2^{p-1}KN(p-1) - 8^{p-1}.$$

3.5.22. As we discussed already, like Carol and Kynèa numbers, Mersenne numbers have very special binary representation; in fact,

- *in binary, the nth Mersenne number consists from $n-1$ unities*:

$$M_n = 2^n - 1 = 2^{n-1} + 2^{n-2} + \cdots + 2^1 + 1 = \sum_{i=0}^{n-1} 2^i.$$

It means that any Mersenne number is a *repunit* in binary; so, in binary, it gives a simplest example of *palindromic number*, i.e., a number that remains the same when its digits are reversed.

Moreover, any Mersenne prime gives a *binary palindromic prime* (i.e., a prime which is palindromic in binary).

Recall (see, for example, [Deza21], Chapter 2, Section 2.5) that the sequence of binary palindromic primes begins (in binary) from 11, 101, 111, 10001, 11111, 1001001, 1101011, 1111111, 100000001, 100111001, … (sequence A117697 in the OEIS) and contains all *Mersenne primes* and all *Fermat primes*.

So, we can state that

- *for any even perfect number, its odd part is a binary palindromic prime, while its even part is an odious number.*

As for *permutable primes*, i.e., prime numbers which, in a given base, can have its digits' positions switched through any permutation and still keeps its primality (see, for example, [Deza21], Chapter 2, Section 2.5), in base 2 only repunits can be permutable primes because any 0 permuted to the last place results in an even number. Therefore,

- *the base* 2 *permutable primes are the only Mersenne primes.*

So, we can state that

- *there exists an one-to-one correspondence between the even perfect numbers and the base 2 permutable primes.*

3.5.23. It is natural to try to generalize primes of the form $2^n - 1$ to primes of the form $b^n - 1$ for $b \neq 2$. However, $b^n - 1$ is always divisible by $b - 1$, so unless the latter is a unit, the former is not a prime. But we can regard a ring of "integers" on complex numbers instead of real numbers.

If we regard the ring $(\mathbb{Z}[i], +, \cdot)$ of *Gaussian integers*,

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}, \qquad \text{where} \quad i^2 = -1,$$

we get the cases $b = 1 + i$ and $b = 1 - i$ and can ask for which n the number $(1 + i)^n - 1$ is a Gaussian prime, which will then be called a *Gaussian Mersenne prime.*

In fact, $(1 + i)^n - 1$ is a Gaussian prime for $n = 2$, 3, 5, 7, 11, 19, 29, 47, 73, 79, ... (sequence A057429 in the OEIS).

Like the sequence of exponents for usual Mersenne primes, this sequence contains only (rational) prime numbers. As for all Gaussian primes, the norms (that is, squares of absolute values) of these numbers are rational primes 5, 13, 41, 113, 2113, 525313, 536903681, 140737471578113, ... (sequence A182300 in the OEIS).

For definition of *Gaussian perfect numbers*, we should now construct the sum of divisors function $\sigma_{\mathbb{Z}[i]}(a + bi)$ in the ring $(\mathbb{Z}[i], +, \cdot)$

of Gaussian integers and choose an analogue of classical condition $\sigma(n) = 2n$ for ordinary (rational) perfect numbers.

In the case of an acceptable choice, one can obtain for Gaussian perfect numbers an analogue of Euclid–Euler theorem. (see, for example, [Spir18] and [McDa74]).

It is possible also to use a similar approach for the construction of *Eisenstein Mersenne primes* and *Eisenstein perfect numbers* in the ring $(\mathbb{Z}[\omega], +, \cdot)$ of *Eisenstein integers*,

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}, \qquad \text{where } \omega = \frac{-1 + i\sqrt{3}}{2}.$$

Here, we get the cases $b = 1 + \omega$ and $b = 1 - \omega$. So, we can ask for what n the number $(1 + \omega)^n - 1$ is an Eisenstein prime, which will then be called an *Eisenstein Mersenne prime*.

In fact, $(1 + \omega)^n - 1$ is an Eisenstein prime for $n = 2$, 5, 7, 11, 17, 19, 79, 163, 193, 239,... (sequence A066408 in the OEIS). The norms (that is, squares of absolute values) of these Eisenstein primes are (rational) primes: 7, 271, 2269, 176419, 129159847, 1162320517, ... (sequence A066413 in the OEIS).

For more information about the construction of the sum of divisors function $\sigma_{\mathbb{Z}[\omega]}(a + b\omega)$ in the ring $(\mathbb{Z}[\omega], +, \cdot)$ of Eisenstein integers, and the choice of an analogue of classical condition $\sigma(n) = 2n$ for ordinary (rational) perfect numbers, which allows to obtain for Eisenstein perfect numbers an analogue of Euclid–Euler theorem, see, for example, [Smal02].

Perfect numbers and Fermat numbers

3.5.24. A *Fermat number*, F_n, is a positive integer of the form

$$F_n = 2^{2^n} + 1, \ n \in \mathbb{Z}, \ n \geq 0.$$

The first Fermat numbers are $3, 5, 17, 257$, $65537, 4294967297$, $18446744073709551617, \ldots$ (sequence A000215 in the OEIS).

In connection with our consideration, it can be proved (Luca, 2000) that

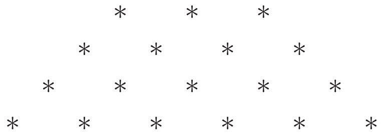
- *a Fermat number cannot be a perfect number or part of a pair of amicable numbers.*

□ For example, for even perfect numbers, it is obvious. As for odd perfect numbers, we can consider F_n modulo 12 and modulo 36 for checking, that F_n is not equal to 1 modulo 12 (in fact, $F_n \equiv 5(mod\ 12)$ for $n \geq 1$) as well as is not equal 9 modulo 36 (in fact, $F_n \equiv 5, 17(mod\ 36)$). As any odd perfect number is equal 1 modulo 12 or is equal 9 modulo 36 (see Section 3.2), we have proven that a Fermat number cannot be an odd perfect number. □

3.5.25. There exists an interesting connection between even perfect numbers, Fermat numbers, and the so-called *trapezoidal numbers.*

An positive integer is called a *trapezoidal number* if it can be represented as some isosceles trapezoid.

For example, a trapezoidal representation of 18 is given by the following picture.



The first few trapezoidal numbers are 5, 7, 9, 11, 12, 13, 14, 15, 17, 18, ... (sequence A165513 in the OEIS).

By definition, any trapezoidal number is a sum of two or more consecutive positive integers greater than 1:

$$Tr(n,k) = n + (n+1) + (n+2) + \cdots + (n + (k-1)),\ n \neq 1,\ k \neq 1.$$

So, one obtains that *any trapezoidal number is a difference of two non-consecutive triangular numbers*:

$$\begin{aligned} Tr(n,k) &= n + (n+1) + (n+2) + \cdots + (n + (k-1)) \\ &= (1 + 2 + \cdots + (n + (k-1))) - (1 + 2 + \cdots + (n-1)) \\ &= S_3(n+k-1) - S_3(n-1). \end{aligned}$$

Moreover, the above definition implies that *any trapezoidal number is a particular case of polite number.*

In fact, a *polite number* is a positive integer that can be represented as the sum of two or more consecutive positive integers.

So, if such *polite representation* starts with 1, we obtain a triangular number, otherwise one gets a trapezoidal number.

The first polite numbers are 1, 3, 5, 6, 7, 9, 10, 11, 12, 13,... (sequence A138591 in the OEIS).

Obviously, a given positive integer can have several polite representations. In the case of 18, one more such representation is given as follows.

* * * * *
* * * * * *
* * * * * * *

The *politeness* of a positive integer number is the number of ways it can be expressed as a sum of consecutive positive integers.

It is easy to show that

- *for any positive integer x, the politeness of x is equal to the number of odd divisors of x that are greater than one.*

□ In fact, suppose a number x has an odd divisor $y > 1$. Then, y consecutive integers, centered on $\frac{x}{y}$ (so that their average value is $\frac{x}{y}$), have x as their sum:

$$x = \left(\frac{x}{y} - \frac{y-1}{2}\right) + \cdots + \frac{x}{y} + \cdots + \left(\frac{x}{y} + \frac{y-1}{2}\right).$$

Some of the terms in this sum may be zero or negative. However, if a term is zero, it can be omitted, and any negative terms may be used to cancel positive ones, leading to a polite representation of x. The requirement that $y > 1$ corresponds to the requirement that a polite representation have more than one term. For instance, the polite number $x = 18$ has two non-trivial odd divisors, 3 and 9. It is therefore the sum of three consecutive numbers centered at $\frac{18}{3} = 6$: $18 = 5 + 6 + 7$. On the other hand, it is the sum of nine consecutive integers centered at $\frac{18}{9} = 2$: $18 = (-3)+(-1)+0+1+2+3+4+5+6$ or $18 = 3 + 4 + 5 + 6$.

Conversely, every polite representation of x can be formed by this construction. If a representation has an odd number y of terms, then the middle term can be written as $\frac{x}{y}$, and $y > 1$ is a non-trivial odd divisor of x. If a representation has an even number $2l$ of terms and its minimum value is m, it may be extended, in a unique way, to a longer sequence with the same sum and an odd number $y = 2(m+l)-1$ of terms, by including the $(2m-1)$ numbers $-(m-1)$, $-(m-2)$,…, -1, 0, 1,…, $m-2$, $m-1$. After this extension, the middle term of the new sequence can be written as $\frac{x}{y}$, and $y > 1$ is a non-trivial odd divisor of x. By this construction, the polite representations of a number and its odd divisors greater than 1 may be placed into a one-to-one correspondence that completes the proof. □

From this consideration, it follows that the *impolite numbers*, i.e., positive integers which are not polite are exactly the powers of two.

So, the first few impolite numbers are 1, 2, 4, 8, 16, 32, 64, 128, 256, 512,… (sequence A000079 in the OES), and the politeness of the numbers 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,… is 0, 0, 1, 0, 1, 1, 1, 0, 2, 1,… (sequence A069283 in the OEIS).

Therefore, the only polite numbers that may be non-trapezoidal are the triangular numbers with only one non-trivial odd divisor because for those numbers, according to the bijection described above, the odd divisor corresponds to the triangular representation and there can be no other polite representation.

Thus, polite non-trapezoidal numbers must have the form of a power of two multiplied by a prime number.

It is easy to show that *there are exactly two types of triangular numbers with this form*:

- *the even perfect numbers* $2^{k-1}(2^k-1)$ *formed by the product of a Mersenne prime* 2^k-1 *with half the nearest power of two*;
- *the products* $2^{k-1}(2^k+1)$ *of a Fermat prime* $2^k+1 = 2^{2^n}+1$ *with half the nearest power of two.*

□ Indeed, if we have the equality $\frac{n(n+1)}{2} = 2^{k-1}\cdot p$ with odd prime number p, then $n(n+1) = 2^k \cdot p$, and hence, $p|n(n+1)$. So, we get that either $p|n$ or $p|(n+1)$.

If $p|n$, then by elementary arguments, $p = n$ and $2^k = n+1$. Therefore, it holds that $p = 2^k - 1$, i.e., p is a Mersenne prime, and the corresponding triangular number $2^{k-1}(2^k-1)$ is an even perfect number.

If $p|(n+1)$, then by elementary arguments, $p = n+1$ and $2^{t+1} = n$. Hence, it holds that $p = 2^{t+1}+1$, i.e., $p = 2^{2^n}+1$ is a Fermat prime, and the corresponding triangular number $2^{k-1}(2^k+1)$ has the form $2^{2^n-1}(2^{2^n}+1)$. □

So, we have proven that *there are only three types of non-trapezoidal numbers*:

- *the even perfect numbers* $2^{k-1}(2^k-1)$ *formed by the product of a Mersenne prime* 2^k-1 *with half the nearest power of two*;
- *the products* $2^{2^n-1}(2^{2^n}+1)$ *of a Fermat prime* $2^{2^n}+1$ *with half the nearest power of two*;
- *powers of two, in particular, all numbers of the form* M_n+1*, where* M_n *is the nth Mersenne number, and all numbers of the form* F_n-1*, where* F_n *is the nth Fermat number.*

Perfect numbers and figurate numbers

3.5.26. The nth *triangular number* $S_3(n)$ is the number of dots in the triangular arrangement with n dots on each side and is equal to the sum of the n positive integers from 1 to n. As the sum of the first n positive integers, $S_3(n) = \frac{n(n+1)}{2}$.

The sequence of triangular numbers, starting with the zeroth triangular number, is 0, 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105, ... (sequence A000217 in the OEIS).

As well as having the form $2^{p-1}(2^p-1) = \frac{(2^p-1)2^p}{2}$, *each even perfect number is the* (2^p-1)*th triangular number*, and hence *is equal to the sum of the integers from 1 to* 2^p-1:

$$2^{p-1}(2^p-1) = S_3(2^p-1) = 1+2+3+\cdots+(2^p-1)\,.$$

For example, $6 = 1+2+3$; $28 = 1+2+3+4+5+6+7$; $496 = 1+2+3+\cdots+31$; $8128 = 1+2+3+\cdots+127$.

3.5.27. The nth *hexagonal number* $S_6(n)$ is defined as the number of distinct dots in a pattern of dots consisting of the outlines of regular hexagons with sides up to n dots when the hexagons are overlaid so that they share one vertex. In other words,

$$S_6(n) = 1+5+9+\cdots+(4n-3) = n(2n-1).$$

Now, it is obvious that

- *the even perfect number* $2^{p-1}(2^p - 1)$ *is the* 2^{p-1}*th hexagonal number*:

$$2^{p-1}(2^p - 1) = S_6(2^p).$$

As an hexagonal number,

- *an even perfect number can be represented as a sum of the first* 2^{p-1} *elements of arithmetic progression* $1, 5, 9, \ldots$:

$$2^{p-1}(2^p - 1) = \sum_{k=0}^{n-1}(4k + 1) \quad \textit{with} \quad n = 2^{p-1}.$$

For example, $6 = 1 + 5$; $28 = 2^2(2^3 - 1)$;

$$\begin{aligned} 496 &= 1 + 5 + 9 + 13 + 17 + 21 + 25 + 29 + 33 + 37 + 41 \\ &\quad + 45 + 49 + 53 + 57 + 61; \\ 8128 &= 1 + 5 + 9 + 13 + 17 + 21 + 25 + 29 + 33 + 37 + 41 \\ &\quad + 45 + 49 + \cdots + 245 + 249 + 253. \end{aligned}$$

3.5.28. Furthermore, a *centered nonagonal number* (or *centered enneagonal number*) is a positive integer number that represents a nonagon with a dot in the center and all other dots surrounding the center dot in successive nonagonal layers. The nth-centered nonagonal number is given by the formula

$$\overline{S}_9(n) = 1 + 9 + 18 + \cdots + 9(n - 1) = \frac{(3n - 2)(3n - 1)}{2}.$$

Therefore, we obtain the following result:

- *Each even perfect number except for* 6 *is the* $(\frac{2^p+1}{3})$*th-centered nonagonal number*:

$$2^{p-1}(2^p - 1) = \overline{S}_9(2^{p-1}).$$

3.5.29. On the other hand, we proved in Section 3.3 that

- *any perfect number cannot be a square number.*

Therefore,

- *any perfect number cannot be an biquadratic number* and, in general, cannot be represented as some even power of an integer.

Perfect numbers and Pascal's triangle

3.5.30. The *Pascal's triangle*

$$\begin{array}{c}
\binom{0}{0}=1\\
\binom{1}{0}=1 \quad \binom{1}{1}=1\\
\binom{2}{0}=1 \quad \binom{2}{1}=2 \quad \binom{2}{2}=1\\
\binom{3}{0}=1 \quad \binom{3}{1}=3 \quad \binom{3}{2}=3 \quad \binom{3}{3}=1\\
\binom{4}{0}=1 \quad \binom{4}{1}=4 \quad \binom{4}{2}=6 \quad \binom{4}{3}=4 \quad \binom{4}{4}=1\\
\binom{5}{0}=1 \quad \binom{5}{1}=5 \quad \binom{5}{2}=10 \quad \binom{5}{3}=10 \quad \binom{5}{4}=5 \quad \binom{5}{5}=1\\
\binom{6}{0}=1 \quad \binom{6}{1}=6 \quad \binom{6}{2}=15 \quad \binom{6}{3}=20 \quad \binom{6}{4}=15 \quad \binom{6}{5}=6 \quad \binom{6}{6}=1\\
\vdots \qquad \vdots \qquad \vdots
\end{array}$$

is a number triangle, the sides of which are formed by 1 and any inner entry is obtained by adding the two entries diagonally above. It is formed by *binomial coefficients* $\binom{n}{m}$ or, equivalently, by the numbers C_n^m of *combinations*, i.e., the ways to choose an unordered subset of m elements from a fixed set of n elements.

It is well known that

$$\binom{n}{m} = C_n^m = \frac{n!}{m!(n-m)!}, \; 0 \le m \le n.$$

Using the *binomial formula*

$$(1+x)^n = \binom{n}{0}x^0 + \binom{n}{1}x^1 + \binom{n}{2}x^2 + \cdots + \binom{n}{n-1}x^{n-1} + \binom{n}{n}x^n$$

with $x = 1$, we get the famous property of Pascal's triangle:

- *The sum of the elements of* n*th row of the triangle is equal to* 2^n, $n = 0, 1, 2, \ldots$.

On the other hand, it is now obvious that

- *the sum of all entries of the first n rows of Pascal's triangle is equal to nth Mersenne number M_n.*

□ In fact, the sum of all elements of the ith row of Pascal's triangle is 2^i, $i = 0, 1, 2, 3, \ldots$. Then, the sum of all elements of the first n rows of Pascal's triangle is equal to

$$2^0 + 2^1 + \cdots + 2^{n-1} = 2^n - 1.$$

This concludes the proof. □

In terms of even perfect numbers, we can say now that

- *the even part of any even perfect number is the sum 2^{p-1} of all elements of the $(p-1)$th row of Pascal's triangle, while the odd part of this even perfect number is the sum of all elements of the first p rows of Pascal's triangle, where p is prime number, giving Mersenne prime $M_p = 2^p - 1$.*

In fact, for the first even perfect number 6, its even part 2 is the sum of elements $1, 1$ of the first row of the Pascal's triangle, while its odd part 3 is the sum of elements $1; 1, 1$ of the first two rows. For the second even perfect number 28, its even part 4 is the sum of elements $1, 2, 1$ of the second row of the Pascal's triangle, while its odd part 7 is the sum of elements $1; 1, 1; 1, 2, 1$ of the first three rows. For the third even perfect number 496, its even part 16 is the sum of elements $1, 4, 6, 4, 1$ of the fourth row of the Pascal's triangle, while its odd part 31 is the sum of elements $1; 1, 1; 1, 2, 1;\ 1, 3, 3, 1; 1, 4, 6, 4, 1$ of the first five rows, etc.

3.5.31. The Mersenne numbers arise also in the Sierpiński sieve, given by the representation of Pascal's triangle modulo 2. It is proven (see, for example, [Deza21], Chapter 2, Section 2.5) that for a given prime p, the

- *pth row of Pascal's triangle is divisible by p.*

It means that in the pth row of Pascal's triangle, if p is a prime number, all the terms except the unities are multiples of p.

So, for any Mersenne prime M_p, we get the following property:

- *Given Mersenne prime M_p, the M_pth row of the Pascal's triangle is divisible by M_p.*

In particular, the third row

$$1, 3, 3, 1$$

is divisible by $M_2 = 2^2 - 1 = 3$, the seventh row

$$1, 7, 21, 35, 35, 21, 7, 1$$

is divisible by $M_3 = 2^3 - 1 = 7$, etc.

Considering Pascal's triangle modulo 2, we can find in this construction all even perfect numbers.

In fact, the nth row of Pascal's triangle is divisible by 2 if and only if $n = 2^k$ ([Deza21], Chapter 2, Section 2.5). In this case, all $2^k - 1$ inner entries of the row are even. So, exactly $2^k - 2$ central entries of the next $(2^k + 1)$th row will be even; exactly $2^k - 3$ central entries of the $(2^k + 2)$th row will be even,..., exactly one central element of the $(2^{k+1} - 2)$th row will be even. In this way, we obtain in the Pascal's triangle modulo 2 a black subtriangle, which contains

$$1 + 2 + \cdots + (2^k - 1) = \frac{(2^k - 1)2^k}{2} = 2^{k-1}(2^k - 1)$$

elements. So, for Mersenne prime M_p, the number of the elements in the corresponding black "even subtriangle" will be a perfect number.

Perfect numbers and pernicious numbers

3.5.32. A *pernicious number* is a positive integer such that the *Hamming weight* of its binary representation (i.e., the sum of binary digits) is prime.

The first pernicious number is 3 since $3 = 11_2$ and $1 + 1 = 2$, which is a prime. The next pernicious number is 5 since $5 = 101_2$, followed by 6, 7, and 9 (sequence A052294 in the OEIS).

Owing to their form, $2^{p-1}(2^p - 1)$, every even perfect number is represented in binary form as p ones followed by $p - 1$ zeros;

for example,

$$6_{10} = 2^2 + 2^1 = 110_2;$$

$$28_{10} = 2^4 + 2^3 + 2^2 = 11100_2;$$

$$496_{10} = 2^8 + 2^7 + 2^6 + 2^5 + 2^4 = 111110000_2;$$

$$8128_{10} = 2^{12} + 2^{11} + 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 = 1111111000000_2.$$

Thus, *every even perfect number is a pernicious number.*

3.5.33. It is known that

- *no power of two is a pernicious number.*

□ This is trivially true because powers of two in binary form are represented as a one followed by zeros. So, each power of two has a Hamming weight of one, which is not considered to be a prime. □

On the other hand,

- *every number of the form* 2^n+1 *with* $n > 0$, *including every Fermat number* $F_n = 2^{2^n} + 1$, *is a pernicious number.*

□ This is because the sum of the digits in binary form is 2, which is a prime number. □

3.5.34. There exist some special numbers which are related to the pernicious numbers and in turn are connected with perfect numbers.

So, for example, *odious numbers* are numbers with an odd number of unities in their binary expansion. The first odious numbers are 1, 2, 4, 7, 8, 11, 13, 14, 16, 19, 21, 22, 25, 26, 28, ... (sequence A000069 in the OEIS).

As any even perfect number has prime number of ones in its binary expansion, we can state that

- *any even perfect number greater than* 6 *is an odious number.*

On the other hand, *evil numbers* are numbers with an even number of unities in their binary expansion. This sequence starts from the numbers 0, 3, 5, 6, 9, 10, 12, 15, 17, 18, 20, 23, 24, 27, 29, ... (sequence A001969 in the OEIS).

So, it is obvious that

- *there exists exactly one even perfect number which is an evil number: It is* $6 = 110_2$.

For the detailed proofs of facts, properties, and theorems listed in this section, as well as some additional information, see, for example, in [AkFr09], [AlEr44], [Bond93], [Buch09], [DeDe12], [DeKo13], [Dele98], [Deza17], [Deza18], [Deza21], [Erdo34] [JoLo99], [Laga02], [McDa74], [MSC96], [Nico69], [PeBy70] [Pill43], [Rama00], [Rama15], [Robi84], [Sier55], [Spir18], [Stew54], [Uspe76], and [Wiki22].

Exercises

1. Check that all proper divisors of the first four perfect numbers are abundant. What can be said about "proper" multiples of the first four perfect numbers? Formulate and prove the corresponding proposition.
2. Prove that all numbers $12t, 945t$, $t \in \mathbb{N}$, are abundant.
3. Find all two-digit highly abundant numbers; all two-digit superabundant numbers. Are there perfect numbers which are highly abundant? Are there perfect numbers which are superabundant?
4. Find all one- and two-digit highly composite numbers. Are there perfect numbers which are highly composite?
5. Check that 6 and 28 are practical numbers. Check that $n!$, $n = 1, 2, 3, 4, 5$ and $p_n\#$, $n = 1, 2, 3, 4, 5$ are practical numbers. Find the first three practical Fibonacci numbers.
6. Check that the first four perfect numbers are Ore harmonic numbers.
7. Check that 6 is a centered pentagonal number, i.e., it can be represent with a dot in the center and all other dots surrounding the center in pentagon's layers (see sequence A005891 in the OEIS); 496 is a centered hendecagonal number, i.e., it can be represent with a dot in the center and all other dots surrounding the center in hendecagon's layers (see sequence A069125 in the OEIS). What can be said about 28?

8. Check that 6 can be represented as a pentagonal pyramidal number (see sequence A002411 in the OEIS). What can be said about 28 and about 496?
9. Find the first five Mersenne primes in the Pascal's triangle; find the first five perfect numbers in the Pascal's triangle. Can we find in the Pascal's triangle any even perfect numbers?
10. Prove that, starting with 7, every third Carol number is a multiple of 7. Prove that, starting with 7, every third Kynéa number is a multiple of 7.
11. An (m, k)-*superperfect number* is a positive integer n such that $\sigma^m(n) = kn$. Prove that the first $(2, 2)$-superperfect numbers are 2, 4, 16, 64, 4096, 65536, and 262144.
12. An *Ore number* is a positive integer, n, such that the harmonic mean of all its divisors $H(n) = \frac{\tau(n)}{\sum_{d|n} 1/d}$ is an integer. Check that $H(n) = 1, \frac{4}{3}, \frac{3}{2}, \frac{12}{7}, \frac{5}{3}, 2, \frac{7}{4}, \frac{32}{15}, \frac{27}{13}, \frac{20}{9}$ for $n = 1,\ 2,\ 3, \ldots, 10$, respectively. Prove that the numbers 1, 6, 28, 140, 270, 496, 672, 1638, 2970, 6200, 8128, 8190 are Ore numbers. Prove that any perfect number is an Ore number.

3.6. Open Problems

The following are the two biggest problems in the theory of perfect numbers:

- Are there any odd perfect numbers?
- Are there infinitely many even perfect numbers?

Are there any odd perfect numbers?

3.6.1. It is unknown whether any odd perfect numbers exist, though a variety of results has been obtained.

In fact, odd perfect numbers either do not exist or are rare.

There are a number of results on perfect numbers that are actually quite easy to prove but nevertheless superficially impressive; some of them obviously come under Richard Guy's strong law of small numbers.

For example, any odd perfect number N must satisfy the following conditions (see Section 3.2):

- N is a perfect square times an odd power of a single prime;
- N is divisible by at least nine primes and has at least 75 prime factors, not necessarily distinct;
- N has at least 1500 decimal digits;
- N has a prime divisor greater that 10^8;
- N has a prime divisor less than $e^{4.97401 \cdot 10^{10}}$;
- $N < 2^{4^{k+1}}$, where $k+1$, is the number of distinct prime factors of N;
- N is of the form $N \equiv 1 (mod\ 12)$ or $N \equiv 9 (mod\ 36)$.

In 1496, Lefèvre stated that Euclid's rule gives all perfect numbers, thus implying that *no odd perfect number exists.*

More recently, Pomerance has presented a heuristic argument suggesting that indeed no odd perfect number should exist.

He has constructed a heuristic which gives an upper bound in general for how likely odd perfect numbers are.

When Pomerance first used his heuristic, it was known that the lower bound for odd perfect numbers was 10^{300}; in this case, one gets a likelihood of about 10^{-70} for an odd perfect number to exist.

Now, it is checked that there is no odd perfect number under 10^{1500}, and we can run his argument through to get a heuristic probability that there is an odd perfect number with probability of about 10^{-340}.

In fact, Pomerance's heuristic actually is a bit stronger and can be read as estimating the chance of an odd multiply perfect number of the form $N = pm^2$, where $\sigma(N) = (2^k)N$ for some k. This is relevant since there is also a more general open question of whether the only multiply perfect odd number is 1.

The probability of such a number existing is very small. Unfortunately, we are also very far from proving their non-existence.

3.6.2. In 1948, Ore introduced the concept of harmonic numbers (i.e., the numbers n for which the harmonic mean $H(n) = \frac{n\tau(n)}{\sigma(n)}$ of their positive integer divisors is an integer) and proved that *perfect numbers are also harmonic.*

So, any odd perfect number should be at the same time an odd Ore harmonic number.

Now, there exists the only known odd Ore harmonic number; it is 1.

Ore conjectured that

- *no odd harmonic divisor numbers exist other than* 1.

If the conjecture is true, this would imply the non-existence of odd perfect numbers.

Cohen, Goto, Sibata, and others starting with Ore himself have performed computer searches listing all small harmonic divisor numbers.

From these results, lists are known of all Ore harmonic numbers up to 10^{14} (Cohen (1997) got the bound $2 \cdot 10^9$; Goto and Okeya got the bound 10^{14}), and all Ore harmonic numbers for which the harmonic mean of the divisors is at most 1200 (Cohen (1997) got the bound 131; Goto and Shibata (2004), got the bound 300; Goto and Okeya got the bound 1200). All of such numbers are even.

So, it is checked that

- if n is a nontrivial odd harmonic number, then $H(n) > 1200$;
- if n is a nontrivial odd harmonic number, then $n > 10^{14}$.

Moreover, for the Ore's conjecture, the following theoretical facts are known:

- A prime power is not harmonic.
- A square-free integer which is greater than 6 is not harmonic.
- An integer which is congruent to 3 modulo 4 is not harmonic.
- If n is a product of two prime powers and is harmonic, then n is an even perfect number.
- For any positive integer c, there exist only finitely many numbers n satisfying $H(n) = c$.

3.6.3. Many of the properties proved about odd perfect numbers also apply to *Descartes numbers*, and Nielsen has suggested that sufficient study of those numbers may lead to a proof that no odd perfect numbers exist.

A *Descartes number* is an odd number which would have been an odd perfect number if one of its composite factors were prime. In other words, a Descartes number n has the form $n = m \cdot p$, where m and p are coprime and $2n = \sigma(m) \cdot (p+1)$, in which p is taken as a "spoof" prime.

They are named after Descartes who observed that the number

$$D = 3^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 22021 = (3 \cdot 1001)^2 \cdot (22 \cdot 1001 - 1) = 198585576189$$

would be an odd perfect number if only 22021 were a prime number since the sum of divisors' function for D would satisfy, if 22021 were prime,

$$\begin{aligned}\sigma(D) &= (3^2+3+1) \cdot (7^2+7+1) \cdot (11^2+11+1) \cdot (13^2+13+1) \\ &\quad \cdot (22021+1) \\ &= (13) \cdot (3 \cdot 19) \cdot (7 \cdot 19) \cdot (3 \cdot 61) \cdot (22 \cdot 1001) \\ &= 3^2 \cdot 7 \cdot 13 \cdot 19^2 \cdot 61 \cdot (22 \cdot 7 \cdot 11 \cdot 13) \\ &= 2 \cdot (3^2 \cdot 7^2 \cdot 11^2 \cdot 13^2) \cdot (19^2 \cdot 61) \\ &= 2 \cdot (3^2 \cdot 7^2 \cdot 11^2 \cdot 13^2) \cdot 22021 = 2D,\end{aligned}$$

where we ignore the fact that 22021 is composite: $22021 = 19^2 \cdot 61$.

This example is the only one currently known.

Are there infinitely many even perfect number?

3.6.4. The most important open problem of the theory of perfect numbers is represented by the following question:

- *Are there infinitely many even perfect numbers*?

Equivalently, we could ask:

- *Are there infinitely many Mersenne primes*?

The answer is probably "yes." In fact, consider the *prime number theorem* (1896, independently by Hadamard and de la Vallée Poussin):

$$\pi(x) = \sum_{p \le x} 1 = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

It means that

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

So, by the prime number theorem, the nth prime number is approximately equal to $n \log n$ (more exactly, $cn \log n < p_n < Cn \log n$, where $C > c > 0$ are some positive absolute constants). Then, we can prove that the probability of a "random" number n being prime is at most $\frac{A}{\log n}$ for some positive absolute constant A.

It is easy to see that

$$\frac{A}{\log M_n} > \frac{A}{\log 2^n} = \frac{A}{n \log 2} = \frac{C}{n},$$

where $C = \frac{A}{\log 2}$ is an absolute constant. Summing over all positive integers, we get the following estimation:

$$\sum_{n=1}^{\infty} \frac{A}{\log M_n} > \sum_{n=1}^{\infty} \frac{A}{\log 2^n} = \sum_{n=1}^{\infty} \frac{A}{n \log 2} = \sum_{n=1|}^{\infty} \frac{C}{n} = C \sum_{n=1}^{\infty} \frac{1}{n}.$$

In other words, it is proven that $\sum_{n=1}^{\infty} \frac{A}{\log M_n}$ is greater than a divergent sum $\sum_{n=1}^{\infty} \frac{1}{n}$ (*harmonic series*); so, it seems likely that there are infinitely many Mersenne primes.

However, our reason cannot be used as a proof of infiniteness of the set of Mersenne primes since the Mersenne numbers are not "random."

Lenstra–Pomerance–Wagstaff and Gillies' conjectures

3.6.5. *Lenstra–Pomerance–Wagstaff conjecture* states that there is an infinite number of Mersenne primes; more precisely, it states that

- *the number of Mersenne primes less than x is asymptotically approximated by*

$$e^{\gamma} \cdot \log_2 \log_2 x,$$

where γ is the Euler–Mascheroni constant.

In other words, the number of Mersenne primes with a given exponent p less than x is asymptotically $e^{\gamma} \cdot \log_2 x$.

This means that there should on average be about $e^{\gamma} \cdot \log_2 10 \approx 5.92$ primes p of a given number of decimal digits such that M_p is prime. The conjecture is fairly accurate for the first 40 Mersenne primes, but between 220000000 and 285000000, there are at least 12 rather than the expected number which is around 3.7.

3.6.6. The *Gillies' conjecture* is a conjecture about the distribution of prime divisors of Mersenne numbers; it was formulated by D. B. Gillies in 1964:

- *If $x < y < \sqrt{M_p}$, as $\frac{x}{y} \to \infty$, and $M_p \to \infty$, the number of prime divisors of M_p in the interval $[x, y]$ is Poisson distributed with*

$$mean \;\sim \begin{cases} \log\left(\dfrac{\log y}{log x}\right), & if \;\; x \geq 2p, \\ \log\left(\dfrac{\log y}{\log 2p}\right), & if \;\; x < 2p. \end{cases}$$

He noted that his conjecture would imply that

- the number of Mersenne primes less than x is $\sim \frac{2}{\log 2} \log\log x$;
- the expected number of Mersenne primes M_p with $x \leq p \leq 2x$ is ~ 2;
- the probability that M_p is prime is $\sim \frac{2\log 2p}{p\log 2}$.

The Lenstra–Pomerance–Wagstaff conjecture gives different values,

- the number of Mersenne primes less than x is $\frac{e^{\gamma}}{\log 2} \log\log x$;
- the expected number of Mersenne primes M_p with $x \leq p \leq 2x$ is $\sim e^{\gamma}$;
- the probability that M_p is prime is $\frac{e^{\gamma}\log 2p}{p\log 2}$ if $p \equiv 3(mod\ 4)$, and is $\frac{e^{\gamma}\log 6p}{p\log 2}$ otherwise.

Asymptotically, these values are about 11% smaller.

While Gillies' conjecture remains open, several papers have added empirical support to its validity, including Ehrman's 1964 paper.

New Mersenne conjecture

3.6.7. In connection with the problem of infiniteness of the set of Mersenne primes, mathematicians are very interested in the following question:

- *Is the new Mersenne conjecture true*?

We recall that the *new Mersenne conjecture* of Bateman, Selfridge, and Wagstaff (1989) states that

- *for any odd positive integer p, if any two of the following conditions hold, then so does the third*:

- $p = 2^k \pm 1$ or $p = 4k \pm 3$ for some natural number k (sequence A122834 in the OEIS);
- $2^p - 1$ is a prime (a *Mersenne prime* M_p; sequence A000043 in the OEIS);
- $\frac{2^p+1}{3}$ is a prime (a *Wagstaff prime*; sequence A000978 in the OEIS).

The first odd primes of the form $2^k \pm 1$ or $4^k \pm 3$ are 3, 5, 7, 13, 17, 19, 31, 61, 67, 127, ... (sequence A122834 in the OEIS).

The exponents p which give Mersenne primes are 2, 3, 5, 7, 13, 17, 19, 31, ... (sequence A000043 in the OEIS).

The first few (odd) primes p such that the numbers $\frac{2^p+1}{3}$ are (Wagstaff) primes, are 3, 5, 7, 11, 13, 17, 19, 23, 31, 43, ... (sequence A000978 in the OEIS).

The known numbers p for which all three conditions hold are 3, 5, 7, 13, 17, 19, 31, 61, 127 (sequence A107360 in the OEIS).

It is also a conjecture that

- *no number which is greater than* 127 *satisfies all three conditions.*

As of 2021, all the Mersenne primes up to $2^{82589933} - 1$ are known, and for none of these does the third condition hold except for the ones just mentioned.

R. Lifchitz has shown that the new Mersenne conjecture is true for all positive integers less than or equal to 30402456 by systematically testing all primes for which it is already known that one of the conditions holds. His website documents the verification of results up to this number.

Other open questions

3.6.8. Consider a sequence

$$\begin{aligned} &CC_0 = 2,\ CC_1 = 2^{CC_0} - 1,\ CC_2 \\ &\qquad = 2^{CC_1} - 1,\ CC_3 = 2^{CC_2} - 1, \ldots, CC_{n+1} = 2^{CC_n} - 1, \ldots. \end{aligned}$$

Starting with CC_1, this sequence forms a subset of the set of Mersenne numbers. An open question is:

- *Are all the numbers CC_n primes*?

These numbers grow very quickly. In fact, the numbers

$$\begin{aligned} &CC_0 = 2;\ CC_1 = 2^2 - 1 = 3;\ CC_2 = 2^3 - 1 = 7; \\ &CC_3 = 2^7 - 1 = 127; \\ &CC_4 = 2^{127} - 1 = 170141183460469231731687303715884105727 \end{aligned}$$

are primes. It is unknown if the number

$$CC_5 > 10^{51217599719369681875006054625051616349}$$

is prime. It seems very unlikely that CC_5 (or many of the larger terms) would be prime, so this is no doubt another example of Guy's strong law of small numbers.

Note that if there is even one composite term in this sequences, then all of the following terms are composite too.

3.6.9. One more open question about the behavior (the infiniteness) of some subset of the set of Mersenne numbers is the following:

- *Are there more double Mersenne primes*?

The double Mersenne number MM_n is a Mersenne number of the form

$$MM_n = M_{M_n} = 2^{2^n-1} - 1,\ n \in \mathbb{N}.$$

The first few double Mersenne numbers are $M_{M_1} = 1$, $M_{M_2} = M_3 = 7$, $M_{M_3} = M_7 = 127$, $M_{M_4} = M_{15} = 32767$ (sequence A077586 in the OEIS).

An early misconception was that

- *if $n = M_p$ is prime, then so is M_n.*

Indeed, each of the first four such numbers is prime:

$$MM_2 = 2^3 - 1 = 7;$$
$$MM_3 = 2^7 - 1 = 127;$$
$$MM_5 = 2^{31} - 1 = 2147483647;$$
$$MM_7 = 2^{127} - 1 = 170141183460469231731687303715884105727.$$

However, the next four ($MM_{13}, MM_{17}, MM_{19}$, and MM_{31}) all have known factors and so are composite.

One more question:

- *Are there any more primes in this sequence*?

Probably not, but it remains an open question.

Note that the sequence of numbers $CC_n, n = 2, 3, 4, \ldots$ discussed above is a subsequence of the sequence of the double Mersenne numbers, and a positive answer to the question of primality of these numbers will give a positive answer to the questions regarding the numbers MM_p.

3.6.10. Besides the problem of the infiniteness of the set of Mersenne primes, we have an important open question about the infiniteness of Mersenne composites:

- *Are there infinitely many composite Mersenne numbers M_p with prime indexes*?

We have shown in Section 3.4 that if $p = 4k + 3$ and $2p + 1$ are primes (in fact, a *Sophie Germain prime* and a *safe prime*, correspondingly), then the Mersenne number $2^p - 1$ is composite because it has a prime divisor $2p + 1$.

As it seems reasonable to conjecture that *there are infinitely many primes pairs* $(p, 2p + 1)$, we can expect that

- *there are infinitely many composite Mersenne numbers M_p with prime index p.*

Sophie Germain primes and safe primes have applications in public-key cryptography and primality testing. Two distributed computing projects, *PrimeGrid* and *Twin Prime Search*, include searches for large Sophie Germain primes.

The largest known Sophie Germain prime (as of 2021) is $137211941292195 \cdot 2^{171960} - 1$ (Járai *et al.*, 2006). It has 51780 digits.

However, the conjecture "*there are infinitely many Sophie Germain primes*" remains unproven.

3.6.11. Perfect numbers (in fact, superabundant numbers or, more exactly, colossally abundant numbers) are also of interest in connection with the *Riemann hypothesis*. In fact, in 1915, Ramanujan proved that under the assumption of the Riemann hypothesis, the inequality

$$\sigma(n) < e^{\gamma} n \log\log n$$

(the so-called *Robin's inequality*) holds for all sufficiently large n.

This inequality is known to fail for 27 numbers (sequence A067698 in the OEIS): 2, 3, 4, 5, 6, 8, 9, 10, 12, 16, 18, 20, 24, 30, 36, 48, 60, 72, 84, 120, 180, 240, 360, 720, 840, 2520, and 5040. The largest known value that violates the inequality is 5040, a superabundant (in fact, a collossally abundant) number.

In 1984, Robin proved that the inequality is true for all $n > 5040$ if and only if the Riemann hypothesis is true.

For some additional information, see, for example, in [AkFr09], [Buch09], [BSW89], [Call92], [Cohe97], [Deza17], [DeKo18], [Dick05], [Ehrm67], [Garc54], [Guy94], [Ingh32], [Kano57], [Kara83], [Pome73], [PoLu10], [Rama00], [Robi84], [Sier64], [Titc87], and [Wiki22].

Exercises

1. Prove that if p is an odd composite number, then $2^p - 1$ and $\frac{2^p+1}{3}$ are both composite.
2. Check that for the numbers 3, 5, 7, 13, 17, 19, 31, 61, and 127, all three conditions of the new Mersenne conjecture hold.
3. Check that the numbers 2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 43, 61, 67, 79, and 89 satisfy at least one condition of the new Mersenne conjecture.
4. Find the first four "double even perfect" numbers, e.g., the perfect numbers, which are produced by double mersenne primes $MM_n = M_{M_n} = 2M_n - 1$.

References

[Apos86], [Avan67], [Bond93], [BSW89], [Buch09], [Call92], [Cohe97], [CoGu96], [DeDe12], [Deza17], [Deza18], [DeKo18], [Deza21], [Dick05], [Diop74], [Ehrm67], [Garc54], [Gard61], [Gard88], [Gill64], [Wief09], [Guy94] [HaWr79], [Ingh32], [Kano57], [Kara83], [Lagr70], [Lege79], [Luca75], [Hogg69], [Pasc54], [Pome73], [Ribe96], [Ries94], [PoLu10], [Rama00], [SlPl95], [Sloa22], [Shan93], [Sier64], [Titc87], [Weis22], and [Wiki22].

This page intentionally left blank

Chapter 4

Amicable Numbers

4.1. History of the Question

4.1.1. Many ancient cultures were concerned with the relationship of a number with the sum of its divisors, often giving mystic interpretations. In Chapter 3, we also considered one such relationship, perfect numbers. In this chapter, we consider another important class of numbers, constructed using the properties of their divisors.

A *pair of amicable numbers* (or an *amicable pair*) is formed by two different positive integers related in such a way that the sum of the proper divisors of each is equal to the other number.

The smallest pair of amicable numbers is $(220, 284)$. They are amicable because the proper divisors of 220 are 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, and 110, whose sum is 284:

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 4 + 55 + 110 = 284;$$

and the proper divisors of 284 are 1, 2, 4, 71, and 142, whose sum is 220:

$$1 + 2 + 4 + 71 + 142 = 220.$$

The first few amicable pairs are: (220, 284), (1184, 1210), (2620, 2924), (5020, 5564), (6232, 6368), (10744, 10856), (12285, 14595), (17296, 18416), (63020, 76084), and (66928, 66992), ... (sequence A259180 in the OEIS; also see A002025 and A002046). It is unknown if there are infinitely many pairs of amicable numbers.

The notion of amicable numbers is a generalization of the notion of *perfect numbers*: Any perfect number which is a number that equals the sum of its own proper divisors and so can be considered as amicable to itself, thus any perfect numbers form an “amicable” pair with equal elements. So, we get degenerate amicable pairs $(6, 6)$, $(28, 28)$, $(496, 496)$, $(8128, 8128)$, etc.

On the other hand, the notion of amicable numbers is a particular case of the notion of *sociable numbers*: a *k-tuple of sociable numbers* is formed by k positive integers related in such a way that the sum of the proper divisors of the first number is equal to the second number, the sum of the proper divisors of the second number is equal to the third number, . . ., the sum of the proper divisors of the last (kth) number is equal to the first number.

In other words, any perfect number forms an *aliquot sequence* of period 1, a pair of amicable numbers constitutes an aliquot sequence of period 2, while a *k-tuple of sociable numbers* forms an aliquot sequence of period k.

4.1.2. Amicable numbers were discovered later than the perfect numbers, probably in the period of the Neoplatonic mystical school (AD third century) of Greek philosophers.

However, Iamblichus of Chalis, a Syrian Neoplatonist philosopher of Arab origin (circa AD 245–325) ascribes (circa AD 320) the knowledge of amicable numbers to the earliest Pythagorean school (circa 500 BC).

In Arabic mathematical writings, the amicable numbers occur repeatedly. They play a role in magic and astrology, in the casting of horoscopes, in sorcery, in the concoction of love potions, and in the making of talismans.

These numbers were mentioned in the *Prolegomena* (1377), a book by the Arab sociologist, philosopher, and historian Ibn Khaldun (1332–1406).

Through the Arabs, the knowledge of amicable numbers spread to Western Europe. They are mentioned in the works of many prominent mathematicians around AD 1500, e.g., French mathematicians Nicolas Chuquet (circa 1445–1500) and Estienne de la Roche (de Villefranche) (1470–1530), the German monk, Protestant reformer, and mathematician Michael Stifel (1487–1567), Italian mathematicians Gerolamo Cardano (1501–1576) and Niccolò Fontana Tartaglia (1500–1557).

Up to this historical period, only a single set of amicable numbers, namely the pair $(220, 284)$, was known. The discovery of the special relationship between the two moderately large numbers for that time is evidence of considerable familiarity with number-theoretic properties.

4.1.3. The first algebraic rule for amicable numbers was invented by in the 9th century by an Arab mathematician, physician, astronomer, and translator Abu-al-Hasan Thābit ibn Qurra (826–901), who lived in Baghdad in the second half of the 9th century and made important discoveries in algebra, geometry, and astronomy. In astronomy, Thābit is considered one of the first reformers of the Ptolemaic system, and in mechanics, he was a founder of statics.

The *Thābit ibn Qurra theorem* states that *if* $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$, *and* $r = 9 \cdot 2^{2n-1} - 1$ *are primes, then* $A = 2^n pq$ *and* $B = 2^n r$ *are amicable.*

This is the first algebraic formula for amicable numbers.

For $n = 2$, it gives the first and the smallest amicable pair, attributed to the legendary Pythagoras.

Two additional pairs (17296, 18416) and (9363584, 9437056) of the Thābit's rule can be obtained for $n = 4$ and $n = 7$ (with no other for $n < 191600$). See the following table for detailed information.

$n = 2$	$n = 4$	$n = 7$
$p = 5$	$p = 23$	$p = 191$
$q = 11$	$q = 47$	$q = 383$
$r = 71$	$r = 1151$	$r = 73727$
$A = 220$	$A = 17296$	$A = 9363584$
$B = 284$	$B = 18416$	$B = 9437056$

In the early 14th century, an Arab mathematician and astronomer, Ibn al-Banna' al-Marrakushi (1256–1321) (also known as Abu'l-Abbas Ahmad ibn Muhammad ibn Uthman al-Azdi) and also

Kamal al-Din Hasan ibn Ali ibn Hasan al-Farisi (1267–1319) (or Abu Hasan Muhammad ibn Hasan) discovered the pair $(17296, 18416)$ corresponding to $n = 4$.

In the 16th century, the Iranian mathematician Muhammad Baqir Yazdi, the last notable Islamic mathematician, discovered the pair (9363584, 9437056) corresponding to $n = 7$.

Much of the work of Eastern mathematicians in this area has been forgotten.

Thābit ibn Qurra's formula was rediscovered by P. Fermat (1601–1665) and R. Descartes (1596–1650), to whom it is sometimes ascribed.

According to a statement by Mersenne, P. Fermat in 1636 rediscovered the Thābit's rule and found the pair $(17296, 18416)$, corresponding to the case $n = 4$.

Descartes stated in a letter to Mersenne in 1638 that he had been led to the same rule and gave the third pair of amicable numbers $(17296, 18416)$.

So, before the Euler's time, only three amicable pairs were known.

Pairs	Time	Authors
(220, 284)	≈500 BC	Pythagoras
(17296, 18416)	≈AD 1300	al-Banna, Farisi, Fermat (1636)
(9363584, 9437056)	≈AD 1600	Yazdi, Descartes (1638)

4.1.4. Leonard Euler (1707–1783) was the first to systematically study amicable numbers. He developed several methods for generating amicable pairs and discovered 59 new pairs.

In 1747, he published a list of 30 pairs but did not reveal his method fully until his elaborate paper *De Numeris Amicabilibus* of 1750 [Eule50]. In this paper, 61 new pairs where listed. But K. Hunrath in 1909 found one to be false, and in 1914, F. Rudi found another false pair.

The basic idea of Euler's methods is to find an amicable pair (EM, EN) with a given common factor E, coprime to the unknown M and N. Since E is given, the sum of divisors of E can be computed. For such a choice, we get that numbers M and N have equal sums of divisors, and one can try to find pairs of numbers under this condition.

Euler considered various combinations of variables in M and N. The simplest choice leading to an amicable pair is $M = pq$ and $N = r$, where p, q, and r are distinct primes of the form

$$p = 2^m(2^k + 1) - 1,\ q = 2^m(2^{2k} + 2^k) - 1,$$
$$r = 2^{2m}(2^{2k+1} + 2^{3k} + 2^k) - 1.$$

If $k = 1$, we obtain

$$p = 3 \cdot 2^m - 1,\ q = 3 \cdot 2^{m+1} - 1,\ r = 9 \cdot 2^{2m+1} - 1,$$

which leads to Thābit's rule.

Rewriting k as $k = n - m$, we get the classical *Euler's rule*; it states that *if*

$$p = 2^m \cdot (2^{n-m} + 1) - 1,\ q = 2^n \cdot (2^{n-m} + 1) - 1,$$
$$r = 2^{m+n} \cdot (2^{n-m} + 1)^2 - 1,$$

where $n > m > 0$ *are integers and* p, q, *and* r *are prime numbers, then* $A = 2^n pq$ *and* $B = 2^n r$ *form a pair of amicable numbers.*

In this notation, the Thābit ibn Qurra theorem corresponds to the case $m = n - 1$.

Euler's rule creates additional amicable pairs for $(m, n) = (1, 8), (29, 40)$ with no others being known.

A.-M. Legendre and P. L. Chebyshev studied the case $k = 7$ for the conditions $p = 2^m(2^k + 1) - 1,\ q = 2^m(2^{2k} + 2^k) - 1,\ r = 2^{2m}(2^{2k+1} + 2^{3k} + 2^k) - 1$. For $m = 1$, they found the amicable pair

$$(2172649216 = 2^8 \cdot 257 \cdot 33023, 2181168896 = 2^8 \cdot 8520191).$$

A. M. Gererdin considered several other values of k, m but found no new amicable pairs.

A 16-year-old Italian schoolboy, Nicolo Paganini, found in 1866 the second smallest pair of amicable numbers $(1184 = 2^5 \cdot 37, 1210 = 2 \cdot 5 \cdot 11^2)$, having been overlooked by earlier mathematicians.

P. Seelhoff found two new pairs in 1884. He used factorization method and may have been the first to take advantage of the more extensive prime tables compiled in the 19th century.

L. E. Dickson discovered two new pairs in 1911 when he completed the examination of a case left unfinished by Euler.

Prime tables did not extend beyond 10^5 in Euler's time, but by 1909, Lehmer's factor table up to 10^7 had been published.

T. E. Mason in 1921 found 14 new amicable pairs.

P. Poulet was the first to use the powerful modern primality testing method developed by Lucas in 1875. He described his application of factorization methods to the search for amicable numbers and claimed to find 108 new amicable pairs (in fact, 104; four pairs were later found to be false). It was a new record after L. Euler.

M. A. Gerardin applied indeterminate analysis systematically as early as 1906 when he explored the forms $(2^2 \cdot 5 \cdot p, 2^2 \cdot q \cdot r)$ and $(2^4 \cdot 23 \cdot p, 2^4 \cdot q \cdot r)$ without finding new pairs. But later, he found five new pairs and was the first to develop methods for exotic amicable pairs and found four pairs of this type. Gererdin also found four amicable pairs jointly with Poulet.

E. B. Escott (1934) was the most prolific discoverer of amicable numbers before the computer era. He made an extensive application of factorization methods to several forms of pairs, some not studied before, and found 233 new pairs, although among them, 14 were later found to be false.

B. H. Brown, in 1939, knowing only Euler's and Paganini's exotic pairs, which contain even numbers, found an exotic pair $(12285 = 3^3 \cdot 5 \cdot 7 \cdot 13, 14595 = 3 \cdot 5 \cdot 7 \cdot 139)$ with odd entries, which he ascertained to be the least odd amicable pair. Brown's method was a form of indeterminate analysis applied to several simple forms, such as $(M = 3^m \cdot a \cdot p, N = 3^n \cdot q)$, in which for given a and m, the possible values of n, p, and q are determined.

4.1.5. P. Poulet continued to search for amicable pairs and his later discoveries were communicated to N. G. W. Beeger in 1941 and 1942 and published in 1948; 42 new pairs where found.

M. García in 1957 used the unknown common factor method. His list contained 153 new pairs.

H. L. Rolf using the exhaustive numerical method was the first to discover an amicable pair on a computer. He investigated all numbers less than 10^5. He proved that there are 13 such pairs and noted that all of them, except the biggest one, (79750, 88730), were listed by E. B. Escott in 1934. Rolf listed also all mathematicians who got some amicable pairs and noted that in 1964, there were in total about 400 known amicable pairs (in fact, 391 as reported by [Rolf65]).

J. Alanen, O. Ore, and J. Stemple extended the numerical search to 10^6 and discovered eight new amicable pairs.

E. J. Lee discovered new amicable pairs by indeterminate analysis methods programmed for computers, in which 264 new amicable pairs were found.

P. Bratley and J. McKay extended the numerical search to 10^7 in 1968 and found 14 new amicable pairs.

Lee noticed in an investigation of the possible form of even amicable pairs that only the following three pairs, discovered by P. Poulet, had sums divisible by 9:

$$(666030256 = 2^4 \cdot 19 \cdot 331 \cdot 6619, 696630544 = 2^4 \cdot 199 \cdot 331 \cdot 661),$$

$$(4150593232 = 2^4 \cdot 43 \cdot 61 \cdot 98899, 4213181998 = 2^4 \cdot 43 \cdot 859 \cdot 7129),$$

$$(4796703664 = 2^4 \cdot 43 \cdot 67 \cdot 104059, 4855069456 = 2^4 \cdot 43 \cdot 373 \cdot 18919).$$

Lee found eight new even pairs with the same property.

He has also proved that neither member of an even amicable pair can contain the factor 3 (it is the answer to a question posed by H. L. Rolf).

Of the eight new pairs with sums divisible by 9 discovered by Lee, six were of the form

$$(M = E \cdot p \cdot q \cdot r, N = E \cdot p \cdot s \cdot t)$$

and two were of the form

$$(M = E \cdot p \cdot q \cdot r, N = E \cdot s \cdot t \cdot u),$$

where p, q, r, s, t, u are distinct primes, and $p, q, r, s, t, u \equiv 1(mod\ 6)$, $E, \sigma(E) \equiv 1(mod\ 3)$.

Lee also found 121 other new pairs of the form $(M = E \cdot p \cdot q, N = E \cdot r \cdot s)$ with $E < 10^5$.

W. Borho in 1976 discovered 38 new pairs.

A. Wulf discovered several new pairs in his 20-year (1930–1950) investigation.

H. Cohen (1970) and, independently, P. Bratley, F. Lunnon, and J. McKay (1970) took the numerical search to 10^8 announcing 57 new pairs.

In 1972, E. J. Lee and J. S. Madachy published a list containing 1107 amicable pairs known at that time.

In 1986, H. J. J. te Riele proposed an efficient exhaustive numerical search method for amicable pairs. With the aid of this method, 1427 amicable pairs with smaller members below 10^{10} were computed, many being new. In the same year, H. J. J. te Riele, W. Borho, S. Battiato, Y. Hoffmann, and E. J. Lee published a table containing 10455 amicable pair between 10^{10} and 10^{52} known to the authors. In addition, S. Battiato and W. Borho in 1988 found 15 odd amicable pairs, with neither number divisible by 3, between 10^{36} and 10^{73}. These pairs are all having the form

$$(M = a \cdot s_1 \cdot \ldots \cdot s_i, N = a \cdot t_1 \cdot \ldots \cdot t_j),$$

where $a = 5^4 \cdot 7^3 \cdot 11^3 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 61^2 \cdot 97 \cdot 307$. te Riele in 1974 discovered four amicable pairs with 32, 40, 81, and 152 digits. In 1984, he found 14 new large amicable pairs between 10^{123} and 10^{282}.

By 1988, the largest known amicable pair was a 1041-digit pair (M, N) of the form

$$(M = 2^9 \cdot p^{20} \cdot p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5,\ N = 2^9 \cdot p^{20} \cdot q_1 \cdot q_2).$$

It was found by H. Wiethaus (Germany).

S. Y. Yan [Yan94] found a new large amicable pair

$$(M = 2^{47} \cdot p \cdot p_1 \cdot p_2,\ N = 2^{47} \cdot p \cdot q_1)$$

in 1993 by using Borho's analogue of Thābit's rule. Both M and N are 65-digit integers. Ninety-five new large amicable pairs have also been found by using the above 65-digit pair as a breeder with an algebraic constructive method.

H. J. J. te Riele has collected all known type-$(i, 1)$, $i = 2, 3, \ldots,$ amicable pairs and counted all daughter pairs which can be constructed from them with the constructive method. From the 234 known type-$(2, 1)$ amicable pairs (which includes the 65-digit pair above), he found 13122 daughter pairs. Moreover, using his new semi-numerical method, te Riele found 116 new amicable pairs (M, N) with $4 \cdot 10^{11} < M + N < 10^{12}$ as well as many amicable triples.

4.1.6. So, in 1946, there were 390 known pairs, but the advent of computers has allowed the discovery of many thousands since then. Exhaustive searches have been carried out to find all pairs less than a given bound, this bound being extended from 10^8 in 1970, to 10^{10} in 1986, to 10^{11} in 1993, to 10^{17} in 2015, and to 10^{18} in 2016.

There are 13 pairs less than 10^5, 42 pairs less than 10^6, 236 less than 10^8, 1427 less than 10^{10}, 3340 pairs less than 10^{11}, 4316 less than $2.01 \cdot 10^{11}$, and 5001 less than $3.06 \cdot 10^{11}$.

In 1972, 1,108 amicable pairs were known (see the list by Lee and Madachy, [LeMa72]). In 2003, the number of amicable pairs exceeded four million. As of 2021, there are over 1227267785 known amicable pairs.

In the following, we list all pairs less than 10^5.

(220, 284)	Pythagoras	c. 500 BC
(1184, 1210)	Paganini	1866
(2620, 2924)	Euler	1747
(5020, 5564)	Euler	1747
(6232, 6368)	Euler	1750
(10744, 10856)	Euler	1747
(12285, 14595	Broun	1939
(17296, 18416)	al-Banna	c. AD 1300
	Farici	c. AD 1300
	Fermat	1636
(63020, 76084)	Euler	1747
(66928, 66992)	Euler	1750
(67095, 71145)	Euler	1747
(69615, 87663)	Euler	1747
(79759, 88730)	Rolf	1964

The following table summarizes the largest known amicable pairs discovered in recent years.

Digits	Date	Reference
4829	1997	García
8684	2003	Jobling and Walker
16563	2004	Walker *et al.*
17326	2004	Walker *et al.*
24073	2005	Jobling

The biggest known amicable pair (M, N) with two 24073-digit numbers has the form

$$(M = a \cdot S \cdot p^{235} \cdot q_1, N = a \cdot q \cdot p^{235} \cdot q_2),$$

where

$$\begin{aligned} a &= 2 \cdot 5 \cdot 11,\ q_1 = (p+q) \cdot p^{235} - 1,\ q_2 = (p-S) \cdot p^{235} - 1, \\ S &= 37 \cdot 173 \cdot 409 \cdot 2136109 \cdot 257817180192109 \\ &\quad \cdot 68340174428454377539, \\ p &= 925616938247297545037380170207625962997960453644 5121, \\ q &= 210958430218054117679018601985059107680988707437 0 \\ &\quad 25081922673599999. \end{aligned}$$

For detailed analysis related to the problem questions, see, for example, [Rolf65], [LeMa72], [GPR03], and [Yan96]. For references and some additional information, see, for example, [LeMa72], [Brow39], [Lee68], [Lee69], [BLM70], [Borh72], [AOS67], [Cohe70], [Cohe93], [Riel74], [Riel84], [Rolf65], [Rolf67], [BaBo88], [BrMc68], [Dick05], [Wiki22], [Weis22], and [Sloa22].

4.2. Divisor Function and Amicable Numbers

Definition of perfect numbers and divisor functions

4.2.1. An *amicable pair* is formed by two different positive integers related in such a way that the sum of the proper divisors of each is equal to the other number.

The sum of positive integer divisors of a number n, excluding the number itself, is called its *aliquot sum*; so, two positive integers form an amicable pair if the aliquot sum of each number is equal to the other number.

In terms of the *aliquot sum function* (or *restricted divisor function*)

$$s(n) = \sum_{d|n,\ d\neq n} d,\ \ n \in \mathbb{N},$$

giving the sum of all *proper divisors* of a positive integer n, i.e., all positive integer divisors of n other than n itself, the classical definition of an amicable pair (M, N) takes the form

$$s(M) = N \ \text{ and } \ s(N) = M.$$

For instance, the proper divisors of 220 are 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, and 110; so,

$$s(220) = 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 4 + 55 + 110 = 284;$$

the proper divisors of 284 are 1, 2, 4, 71, and 142, and

$$s(284) = 1 + 2 + 4 + 71 + 142 = 220.$$

So, we get an amicable pair $(220, 281)$ because

$$s(220) = 284, \ \text{ while } \ s(284) = 220.$$

While the ancient Greeks originally defined amicable numbers in terms of the sum of the proper divisors, it is more convenient for most purposes to define a pair of positive integers (M, N) in terms of the sum of divisors function

$$\sigma(n) = \sum_{d|n} d,\ \ n \in \mathbb{N},$$

giving the sum of all positive integer divisors of a positive integer n, including n itself. By definition, $\sigma(n) = s(n) + n$, so in terms of the sum of divisors function, a pair of positive integers (M, N) is called perfect if they satisfy the condition

$$\sigma(M) = N + M = \sigma(N).$$

In this case, the number $N + M$ is called the *sum of pair.* For instance,

$$\sigma(220) = 1+2+4+5+10+11+20+22+4+55+110+220 = 504,$$

$$\sigma(284) = 1 + 2 + 4 + 71 + 142 + 284 = 504,$$

and we obtain an amicable pair $(220, 281)$ with the sum of pair 504:

$$s(220) = 220 + 284 = \sigma(284).$$

Much of the study of amicable numbers relies on the fact that $\sigma(n)$ is a multiplicative function.

4.2.2. The sums of divisors produce various other kinds of numbers.

Numbers n for which $s(n) = n$ or $\sigma(n) = 2n$ are called *perfect*. They can be considered as amicable to itself (formally, $\sigma(n) = n + n = \sigma(n)$), so any perfect number n form an "amicable" pair (n, n) (formally, $\sigma(n) = n + n = \sigma(n)$).

Numbers n for which $s(n) < n$ or $\sigma(n) < 2n$ are called *deficient*, and where $s(n) > n$ or $\sigma(n) > 2n$, the numbers are called *abundant*.

On the other hand, the notion of amicable numbers is a particular case of the notion of *sociable numbers*: A *k-tuple of sociable numbers* is formed by k positive integers $(x_1, x_2, \ldots, x_k)$ related in such a way that

$$s(x_1) = x_2,\ s(x_2) = x_3, \ldots, s(x_{k-1}) = x_k,\ s(x_k) = x_1.$$

By definition, for $k = 1$, we get an amicable pair.

In terms of the sigma function, a *k-tuple of sociable numbers* is formed by k positive integers $(x_1, x_2, \ldots, x_k)$ such that

$$\sigma(x_1) = x_1 + x_2,\ \sigma(x_2) = x_2 + x_3, \ldots, \sigma(x_{k-1}) = x_{k-1} + x_k,$$

$$\sigma(x_k) = x_k + x_1.$$

Formally, for a given positive integer n, we define the *aliquot sequence* of n as

$$s^0(n) = n, s^1(n) = s(n), s^2(n) = s(s(n)), \ldots.$$

Then, for any perfect number n, we get the constant sequence $n, n, n, n, \ldots$; for any amicable pair (M, N), we get the sequence $M, N, M, N, \ldots$; for any k-tuple of sociable numbers $(x_1, x_2, \ldots, x_k)$, we get the sequence $x_1, x_2, \ldots, x_k, x_1, x_2, \ldots, x_k, \ldots$. All constructed sequences are periodical: Any perfect number forms an aliquot sequence of period 1, a pair of amicable numbers constitutes an aliquot sequence of period 2, while a k-tuple of sociable numbers forms an aliquot sequence of period k, $k \geq 3$.

For instance, the quadruplet $(1264460, 1547860, 1727636, 1305184)$ gives an example of amicable 4-cycle.

In fact, the sum $s(1264460)$ of the proper divisors of $1264460 = 2^2 \cdot 5 \cdot 17 \cdot 3719$ is

$$\begin{aligned} &1 + 2 + 4 + 5 + 10 + 17 + 20 + 34 + 68 + 85 + 170 + 340 + 3719 \\ &\quad + 7438 + 14876 + 18595 + 37190 + 63223 + 74380 + 126446 \\ &\quad + 252892 + 316115 + 632230 = 1547860; \end{aligned}$$

the sum $s(1547860)$ of the proper divisors of $1547860 = 2^2 \cdot 5 \cdot 193 \cdot 401$ is

$$\begin{aligned} &1 + 2 + 4 + 5 + 10 + 20 + 193 + 386 + 401 + 772 + 802 + 965 \\ &\quad + 1604 + 1930 + 2005 + 3860 + 4010 + 8020 + 77393 + 154786 \\ &\quad + 309572 + 386965 + 773930 = 1727636; \end{aligned}$$

the sum $s(1727636)$ of the proper divisors of $1727636 = 2^2 \cdot 521 \cdot 829$ is

$$\begin{aligned} &1 + 2 + 4 + 521 + 829 + 1042 + 1658 + 2084 + 3316 \\ &\quad + 431909 + 863818 = 1305184; \end{aligned}$$

lastly, the sum $s(1305184)$ of the proper divisors of $1305184 = 2^5 \cdot 40787$ is

$$\begin{aligned} &1 + 2 + 4 + 8 + 16 + 32 + 40787 + 81574 + 163148 \\ &\quad + 326296 + 652592 = 1264460. \end{aligned}$$

It is easy to see that sociable numbers give a generalization of amicable numbers, while perfect numbers can be considered as a particular case of amicable pairs with two equal elements.

Using other approaches, we can get many interesting classes of special numbers (*amicable n-tuples*, *multi-amicable pairs*, *friendly numbers*, etc.), closely connected with amicable numbers and having arithmetical properties, depending on the structure of their positive integer divisors.

We consider many such classes of numbers in Section 4.5 of this chapter and, especially, in Chapter 5.

4.2.3. For further consideration, we need some additional definitions.

Let (M, N) be a pair of amicable numbers with $M < N$, and write $M = gm$ and $N = gn$, where $g = gcd(M, N)$ is the greatest common divisor of M and N. If m and n are both coprime to g and square-free, then the pair (M, N) is said to be *regular*; otherwise, it is called *irregular* (or *exotic*).

If the amicable pair (M, N), $M < N$, is regular and M and N have i and j prime factors, respectively, then the pair (M, N) is said to be of *type*-(i, j).

For example, for the first amicable pair

$$(220, 284) = (2^2 \cdot 5 \cdot 11, 2^2 \cdot 71),$$

the greatest common divisor $g = gcd(220, 284)$ is 4, and so, $m = 55 = 5 \cdot 11$ and $n = 71$. Therefore, the pair $(220, 284)$ is regular of type-$(2, 1)$.

For the second amicable pair

$$(1184, 1210) = (2^5 \cdot 37, 2 \cdot 5 \cdot 11^2),$$

the greatest common divisor $g = gcd(1184, 1210)$ is 2, so $m = 592$ and $n = 605$. As m is not coprime to g (and moreover not square-free), the pair $(1184, 1210)$ is exotic.

Thābit ibn Qurra theorem

4.2.4. The *Thābit ibn Qurra theorem* (or *Thābit's rule*) is a method for discovering amicable numbers invented in the 9th century by the Arab mathematician Thābit ibn Qurra.

Theorem (Thābit ibn Qurra theorem). *If* $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$, *and* $r = 9 \cdot 2^{2n-1} - 1$ *are all primes, then* $(M = 2^n \cdot p \cdot q, N = 2^n \cdot r)$ *is an amicable pair.*

□ We consider two proofs of this theorem.

I. The first proof uses classical definition of amicable pairs due to sums of aliquot parts of the numbers M and N.

Consider all proper divisors of M. They are $1, 2, \ldots, 2^n, p, 2p, \ldots, 2^np, q, 2q, \ldots, 2^nq, pq, 2pq, \ldots, 2^{n-1}pq$. Their sum is

$$\begin{aligned}
s(M) &= (1 + 2 + \cdots + 2^n) + p(1 + 2 + \cdots + 2^n)\\
&\quad + q(1 + 2 + \cdots + 2^n) + pq(1 + 2 + \cdots + 2^{n-1})\\
&= (2^{n+1} - 1)(1 + p + q) + (2^n - 1)pq\\
&= (2^{n+1} - 1)(1 + (3 \cdot 2^{n-1} - 1) + (3 \cdot 2^n - 1))\\
&\quad + (2^n - 1)(3 \cdot 2^{n-1} - 1)(3 \cdot 2^n - 1)\\
&= (2^{n-1} - 1)(9 \cdot 2^{n-1} - 1) + (2^n - 1)(9 \cdot 2^{2n-1} - 9 \cdot 2^{n-1} + 1)\\
&= 2^{n+1} \cdot 9 \cdot 2^{n-1} - 2^{n+1} + 1 + 2^n \cdot 9 \cdot 2^{2n-1}\\
&\quad - 9 \cdot 2^{2n-1} - 9 \cdot 2^{n-1} + 9 \cdot 2^{n-1} + 2^n - 1\\
&= 9 \cdot 2^{2n} - 9 \cdot 2^{2n} + 2^n \cdot 9 \cdot 2^{2n-1} - 2^n = 2^n(9 \cdot 2^{2n-1} - 1) = N.
\end{aligned}$$

Consider all proper divisors of N. They are $1, 2, \ldots, 2^n, r, 2r, \ldots, 2^{n-1}r$. Their sum is

$$\begin{aligned}
s(N) &= 1 + \cdots + 2^n + r(1 + 2 + \cdots + 2^{n-1})\\
&= (2^{n+1} - 1) + (2^n - 1) + (2^n - 1)(9 \cdot 2^{2n-1})\\
&= 2^n \cdot (2 + 9 \cdot 2^{2n-1} - 1) - 9 \cdot 2^{2n-1} + 1 - 1\\
&= 2^n \cdot (9 \cdot 2^{2n-1} + 1) - 9 \cdot 2^{2n-1} = 2^n \cdot (9 \cdot 2^{2n-1} + 1 - 9 \cdot 2^{n-1})\\
&= 2^n \cdot (3 \cdot 2^{n-1} - 1)(3 \cdot 2^n - 1) = 2^npq = M.
\end{aligned}$$

So, $s(M) = n$, $s(N) = M$, and numbers $M = 2^n \cdot p \cdot q$, $N = 2^n \cdot r$ form an amicable pair.

II. The second proof uses the multiplicativity of sigma function and the fact that $\sigma(2^k) = 2^{k+1} - 1$, while $\sigma(p) = p + 1$ for any prime number p. In fact, we have that

$$\begin{aligned} M + N &= 2^n(pq + r) = 2^n((3 \cdot (2^n - 1)(3 \cdot 2n - 1) + (9 \cdot 2^{2n-1} - 1) \\ &= 2^n(9 \cdot 2^{2n-1} - 3 \cdot 2^n - 3 \cdot 2^{n-1} + 9 \cdot 2^{2n-1}) \\ &= 2^n(9 \cdot 2^{2n} - 9 \cdot 2^{n-1}) = 2^n \cdot 9 \cdot 2^{n-1}(2^{n+1} - 1) \\ &= 9 \cdot 2^{2n-1}(2^{n+1} - 1). \end{aligned}$$

On the other hand,

$$\begin{aligned} \sigma(M) &= \sigma(2^n pq) = (2^{n+1} - 1)(p + 1)(q + 1) \\ &\quad = (2^{n+1} - 1) \cdot 3 \cdot 2^{n-1} \cdot 3 \cdot 2^n = 9 \cdot 2^{2n-1}(2^{n+1} - 1) \end{aligned}$$

and

$$\begin{aligned} \sigma(N) &= \sigma(2^n r) = (2^{n+1} - 1)(r + 1) = (2^{n+1} - 1) \cdot 9 \cdot 2^{2n-1} \\ &= 9 \cdot 2^{2n-1}(2^{n+1} - 1). \end{aligned}$$

So, we get that $\sigma(M) = M + N = \sigma(M)$, and hence, the numbers $M = 2^n \cdot p \cdot q$, $N = 2^n \cdot r$ form an amicable pair. □

For $n \leq 2000$, Thābit's rule only generates amicable pairs when $n = 2, 4$, and 7:

$$(220, 284) = (2^2 \cdot 5 \cdot 11, 2^2 \cdot 71);$$
$$(17296, 18416) = (2^4 \cdot 23 \cdot 47, 2^4 \cdot 1151);$$
$$(9363584, 9437056) = (2^7 \cdot 191 \cdot 383, 2^7 \cdot 73727),$$

and no other such pairs are known.

Although we know only three amicable pairs generated by Thābit's rule and, moreover, Thābit himself did not use his rule to find any new amicable pair, it is the first and one of the most important algebraic methods in the theory of amicable pairs. Most of the modern algebraic methods for generating amicable pairs are based on Thābit's rule and its analogues.

Numbers of the form $3 \cdot 2^n - 1$ are known as *Thābit numbers*.

The first few Thābit numbers are 2, 5, 11, 23, 47, 95, 191, 383, 767, 1535, 3071, 6143, 12287, 24575, 49151,... (sequence A055010 in the OEIS).

In order for Thābit's rule to produce an amicable pair, two consecutive Thābit numbers must be prime; this severely restricts the possible values of n.

The first *Thābit primes*, i.e., Thābit numbers which are prime, are 2, 5, 11, 23, 47, 191, 383, 6143, 786431, 51539607551, 824633720831, ... (sequence A007505 in the OEIS).

As of 2021, there are 64 known prime Thābit numbers. Their n-values are: 0, 1, 2, 3, 4, 6, 7, 11, 18, 34, 38, 43, 55, 64, 76, ..., 1232255, 2312734, 3136255, 4235414, 6090515, 11484018, 11731850, 11895718, 16819291, 17748034 (sequence A002235 in the OEIS).

To establish the theorem, Thābit ibn Qurra proved nine lemmas divided into two groups. The first three lemmas deal with the determination of the aliquot parts of a natural integer. The second group of lemmas deals more specifically with the formation of perfect, abundant, and deficient numbers.

Euler's version of Thābit's method

4.2.5. Euler was the first to study amicable numbers systematically. Based on Thābit's rule, he developed several new methods of generating of amicable numbers and found 59 new amicable pairs. Since Euler's time, many more amicable pairs have been found, most of them with the help of various modifications of Thābit's and Euler's methods.

The *Euler's theorem* (*Euler's rule*) for discovering amicable numbers is a generation of the Thābit ibn Qurra theorem.

Theorem (Euler's theorem). *If* $p = 2^m \cdot (2^{n-m}+1) - 1$, $q = 2^n \cdot (2^{n-m}+1) - 1$, $r = 2^{n+m} \cdot (2^{n-m}+1)^2 - 1$ *are all primes, where* $1 \le m \le n-1$, *then* $(M = 2^n \cdot p \cdot q, N = 2^n \cdot r)$ *is an amicable pair.*

Thābit ibn Qurra theorem corresponds to the case $m = n - 1$.

□ Consider

$$\begin{aligned} M + N = 2^n(pq + r) &= 2^n(2^{n+m+1}(2^{n-m}+1)^2 \\ &\quad - (2^n + 2^m)(2^{n-m}+1)) \\ &= 2^{n+m}(2^{n-m}+1)(2^{n+1}(2^{n-m}+1) - (2^{n-m}+1)) \\ &= 2^{n+m}(2^{n-m}+1)^2(2^{n+1}-1). \end{aligned}$$

On the other hand,

$$\begin{aligned}\sigma(M) &= \sigma(2^n pq) = (2^{n+1}-1)(p+1)(q+1)\\ &= (2^{n+1}-1)\cdot 2^m(2^{n-m}+1)\cdot 2^n(2^{n-m}+1)\\ &= 2^{n+m}(2^{n+1}-1)(2^{n-m}+1)^2,\end{aligned}$$

while

$$\begin{aligned}\sigma(N) = \sigma(2^n r)(2^{n+1}-1)(r+1) &= (2^{n+1}-1)\cdot 2^{n+m}(2^{n-m}+1)^2\\ &= 2^{n+m}(2^{n+1}-1)(2^{n-m}+1)^2.\end{aligned}$$

So, $\sigma(M) = M+N = \sigma(N)$, and hence, the numbers $M = 2^n \cdot p \cdot q$ and $N = 2^n \cdot r$ form an amicable pair. ☐

For $m = n-1$, it holds that $p = 2^{n-1}\cdot 3 - 1$, $q = 2^n \cdot 3 - 1$, $r = 2^{2n-1}\cdot 3^2 - 1$, and we can state that Thābit's rule follows from Euler's rule in this case.

4.2.6. Note that Euler's rule gives *all* amicable pairs of the form $(2^n pq, 2^n r)$. In fact,

- *if numbers* $2^n\cdot p\cdot q, 2^n\cdot r$ *with distinct odd primes* p, q, r *form amicable pair, then* $p = 2^{n-l}\cdot g - 1$, $q = 2^n\cdot g - 1$, *and* $r = 2^{2n-1}\cdot g^2 - 1$, *with* $g = 2^l + 1$ *and* $1 \le l \le n-1$.

☐ By the definition of an amicable pair, the numbers n, p, q, r must satisfy the conditions

$$(p+1)(q+1) = r+1, \quad \text{and} \quad (2^{n+1}-1)(p+1)(q+1) = 2^n(pq+r).$$

It follows that

$$r = pq+p+q \quad \text{and} \quad (p-(2^n-1))(q-(2^n-1)) = 2^{2n}.$$

So, we can state that

$$p-(2^n-1) = 2^{n-l} \quad \text{and } q-(2^n-1) = 2^{n+l}$$

for some integer l with $1 \le l \le n-1$, and therefore,

$$p = (2^n-1)+2^{n-l} \quad \text{and } q = (2^n-1)+2^{n+l}.$$

Using the condition $r = pq + p + q$, we get now that

$$p = 2^{n-l}(2^l + 1) - 1,\ q = 2^n(2^l + 1) - 1,$$
$$r = pq + p + q = 2^{2n-l}(2^l + 1)^2 - 1.$$

The above form of Euler's rule can be obtained for $m = n - l$. □

4.2.7. For practical reasons, it is more convenient to formulate Euler's rule in the following algorithmic form (see Section 4.4):

- *For a given positive integer n, choose a positive integer x, $1 \le x \le n-1$; let $g = 2^{n-x} + 1$; if $p = 2^x \cdot g - 1$, $q = 2^n \cdot g - 1$, $r = 2^{n+x} \cdot g^2 - 1$ are all primes, then $(M = 2^n \cdot p \cdot q, N = 2^n \cdot r)$ is an amicable pair.*

□ Since

$$\begin{aligned} M + N &= 2^n(pq + s) = 2^n((2^x g - 1)(2^n g - 1) + 2^{n+x}g^2 - 1)) \\ &= 2^{2n+x}g^2 - 2^{n+x}g - 2^{2n}g + 2^{2n+x}g^2 = (2^{n+1} - 1)2^{n+x}g^2, \\ \sigma(M) &= \sigma(2^n)\sigma(p)\sigma(q) = (2^{n+1} - 1)(2^x g)(2^n g) = (2^{n+1} - 1)2^{x+n}g^2, \\ \sigma(N) &= \sigma(2^n)\sigma(r) = (2^{n+1} - 1)2^{n+x}g^2, \end{aligned}$$

we get that $\sigma(M) = M + N = \sigma(N)$. So, by definition, the numbers $M = 2^n \cdot p \cdot q$ and $N = 2^n \cdot r$ form an amicable pair. □

Euler's rule creates additional amicable pairs for $(m, n) = (1, 8), (29, 40)$ with no others being known. So, there are exactly five pairs obtained by Euler's methods:

n	x	Amicable pair	
$n = 2$	$x = 1$	$(220, 284)$	Pythagoras
$n = 4$	$x = 3$	$(17296, 18416)$	al-Banna, Farisi, Feremat
$n = 7$	$x = 6$	$(9363584, 9437056)$	Yazdi, Descarts
$n = 8$	$x = 1$	$(2172649216, 2181168896)$	Legendre, Chebyshev
$n = 40$	$x = 29$	$(2724918040393706557785752240819405848576,$ $2724918040396184856306258038787235905536)$	te Riele

The biggest pair has 40 digits in each of its numbers. te Riele checked that there are no other such pairs with $n \le 50$.

In 1994, Yan proved ([Yan94]) that

- *Euler's method only gives five amicable pairs for $n \le 1000$.*

So, Thābit's rule gives three pairs of amicable numbers, no more amicable pairs have been generated by this rule for $7 < n < 191600$.

Euler's rule only gives two more pairs than Thābit's. No more amicable pairs have been generated by this rule for $40 < n \leq 1000$.

How Euler obtained his rule

4.2.8. In 1747 and 1750, Euler published two extensive papers, where he proposed five methods of searching for amicable pairs and added 59 new amicable pairs to the three amicable pairs known thus far.

The basic idea of Euler's first four methods is to find an amicable pair (Em, En) with a given common factor E, coprime to the unknown m and n. Since E is given, the sum $S = \sigma(E)$ of divisors of E can be computed. For such a choice, we get that

$$S\sigma(m) = E(m+n) = S\sigma(n),$$

so numbers m and n have equal sums of divisors, $\sigma(m) = \sigma(n)$, and one can try to find pairs of numbers under this condition.

Euler considered various combinations of variables in m and n.

The simplest choice $E = 2^n$, $m = p \cdot q$, $n = r$, where p, q, r are distinct odd primes, leading to the conditions

$$p = 2^m(2^k+1)-1,\ q = 2^m(2^{2k}+2^k)-1,\ r = 2^{2m}(2^{2k+1}+2^{3k}+2^k)-1,$$

i.e., produce Thābit's and Euler's rules, described above.

By choosing $A = 3^2 \cdot 7 \cdot 13$, $m = p \cdot q$, $n = r$, Euler found that the first odd amicable pair

$$(M = 69615 = 3^2 \cdot 7 \cdot 13 \cdot 5 \cdot 17, N = 87633 = 3^2 \cdot 7 \cdot 13 \cdot 107).$$

On the other hand, one can try to find an unknown common factor E if the numbers n and m are given. In fact, Euler considered such an approach by assuming that m and n, satisfying the condition $\sigma(m) = \sigma(n)$ are given, while E is to be found, satisfying the condition

$$\frac{\sigma(E)}{E} = \frac{m+n}{\sigma(m)}.$$

If, moreover, $gcd(E, m) = gcd(E, n) = 1$, then (Em, En) is an amicable pair:

$$\sigma(Em) = \sigma(E)\sigma(m) = E(m + n) = Em + En,$$
$$\sigma(En) = \sigma(E)\sigma(n) = \sigma(E)\sigma(m) = \sigma(Em).$$

García found 153 new amicable pairs with the help of this "unknown common factor" method.

4.2.9. It is interesting to investigate how Euler obtained his rule.

From the Thābit's rule, we know that if we can find three primes of the form

$$p = 3 \cdot 2^{n-1} - 1 \; q = 3 \cdot 2^n - 1, \; r = 9 \cdot 2^{2n-1} - 1,$$

then we can obtain an amicable pair $(M, N) = (2^n \cdot q \cdot p, 2^n \cdot r)$. We also know that

$$\begin{aligned} pq + r &= 9 \cdot 2^{2n-1} - 3 \cdot 2^n - 3 \cdot 2^{n-1} + 9 \cdot 2^{2n-1} \\ &= 9 \cdot 2^{2n} - 9 \cdot 2^{n-1} = 9 \cdot 2^{n-1}(2^{n+1} - 1). \end{aligned}$$

If we let $\alpha_1 = \alpha_1 = 1$ and $\alpha_3 = \alpha_1 + \alpha_2$, then the Thābit 's rule can be rewritten in a slightly more general form as follows:

$$p = 3^{\alpha_1} 2^{n-1} - 1, \; q = 3^{\alpha_2} 2^n - 1, \; r = 3^{\alpha_3} 2^{2n-1} - 1.$$

Now, we try to generalize this idea further by putting $M = 2^k \cdot q$ and $N = 2^k \cdot r$, where

$$p = 3^{\alpha_1} \cdot 5^{\beta_1} \cdot 2^{\gamma_1} - 1, \; q = 3^{\alpha_2} \cdot 5^{\beta_2 \cdot} 2^{\gamma_2} - 1, \; r = 3^{\alpha_3} \cdot 5^{\beta_3} \cdot 2^{\gamma_3} - 1.$$

We suppose that α_i, β_i, γ_i are non-negative integers with $\alpha_1 \leq \alpha_2 \leq \alpha_3$, $\beta_1 \leq \beta_2 \leq \beta_3$, $\gamma_1 < \gamma_2 < \gamma_3$. If p, q, r are all primes, we have

$$\begin{aligned} \sigma(2^k pq) &= (2^{k+1} - 1)(p + 1)(q + 1) \\ &= (2^{k+1} - 1)3^{\alpha_1+\alpha_2} 5^{\beta_1+\beta_2} 2^{\gamma_1+\gamma_2}, \\ \sigma(2^k r) &= (2^{k+1} - 1)(r - 1) = (2^{k+1} - 1)3^{\alpha_3} 5^{\beta_3} 2^{\gamma_3}. \end{aligned}$$

In order for (M, N) to be an amicable pair, we must have

$$\sigma(2^k pq) = \sigma(2^k r).$$

So, in this case, it holds that

$$\alpha_3 = \alpha_1 + \alpha_2,\ \beta_3 = \beta_1 + \beta_2,\ \gamma_3 = \gamma_1 + \gamma_2.$$

Also,

$$\begin{aligned} pq + r &= 3^{\alpha_1+\alpha_2}5^{\beta_1+\beta_2}2^{\gamma_1+\gamma_2} - 3^{\alpha_1}5^{\beta_1}2^{\gamma_1} \\ &\quad - 3^{\alpha_2}5^{\beta_2}2^{\gamma_2} + 3^{\alpha_3}5^{\beta_3}2^{\gamma_3} \\ &= 3^{\alpha_1}5^{\beta_1}2^{\gamma_1}(3^{\alpha_2}5^{\beta_2}2^{\gamma_2} - 1 - 3^{\alpha_2-\alpha_1}5^{\beta_2-\beta_1}2^{\gamma_2-\gamma_1} \\ &\quad + 3^{\alpha_3-\alpha_1}5^{\beta_3-\beta_1}2^{\gamma_3-\gamma_1}) \\ &= 3^{\alpha_1}5^{\beta_1}2^{\gamma_1}(3^{\alpha_2}5^{\beta_2}2^{\gamma_2+1} - 1 - 3^{\alpha_2-\alpha_1}5^{\beta_2-\beta_1}2^{\gamma_2-\gamma_1}). \end{aligned}$$

Since

$$2^k(pq + r) = \sigma(2^k pq)\sigma(2^k r),$$

then

$$k = \gamma_2,\ \alpha_1 = \alpha_2,\ \beta_1 = \beta_2.$$

So,

$$3^{\alpha_2}5^{\beta_2}(2^{\gamma_2+1} - 1 - 2^{\gamma_2-\gamma-1})$$

must be

$$3^{\alpha_2}5^{\beta_2}(2^{\gamma_2+1} - 1).$$

Therefore, we get

$$2^{\gamma_2-\gamma_1} + 1 = 3^{\alpha_2}5^{\beta_2}.$$

I. If we choose $\gamma_2 - \gamma_1 = 1$, then we have $2^1 + 1 = 3^1 \cdot 5^0$. Therefore, $\alpha_1 = \alpha_2 = 1$, $\beta_1 = \beta_2 = 0$, and with $\gamma_2 = \gamma$, we get $M = 2^k \cdot p \cdot q$ and $N = 2^k \cdot r$, where

$$p = 3 \cdot 2^{\gamma-1} - 1,\ q = 3 \cdot 2^{\gamma} - 1,\ r = 3^2 \cdot 2^{2\gamma-1} - 1.$$

This is the Thābit's original rule.

II. Taking $\gamma_2 - \gamma_1 = 2$, we would have $2^2 + 1 = 3^0 \cdot 5^1$. Therefore, $\alpha_1 = \alpha_2 = 0$, $\beta_1 = \beta_2 = 1$, where

$$p = 5 \cdot 2^{\gamma_2-2} - 1,\ q = 5 \cdot 2^{\gamma_2} - 1,\ r = 5^2 \cdot 2^{2\gamma_2-2} - 1.$$

As $r = 5^2 \cdot 2^{2\gamma_2-2} - 1 = (5 \cdot 2^{\gamma_2-1} - 1)(5 \cdot 2^{\gamma_2-1} + 1)$ is always composite, there is no corresponding amicable rule.

III. Taking $\gamma_2 - \gamma_1 = 3$, we would have $2^3 + 1 = 3^2 \cdot 5^0$. Therefore, $\alpha_1 = \alpha_2 = 2$, $\beta_1 = \beta_2 = 0$, where

$$p = 3^2 \cdot 2^{\gamma_2 - 3} - 1,\ q = 3^2 \cdot 2^{\gamma_2} - 1,\ r = 3^4 \cdot 2^{2\gamma_2 - 3} - 1.$$

So, if p, q, r are all primes, then $(M, N) = (2^{\gamma_2} \cdot p \cdot q, 2^{\gamma_2} \cdot r)$ is an amicable pair. This rule seems to be new, although no amicable pairs have been found for $4 \leq \gamma_2 \leq 100$ by numerical computation, as all constructed p, q, r are not simultaneously primes.

4.2.10. We can perform a similar analysis with the products $3^\alpha \cdot 5^\beta$ of 3 and 5 being replaced by products of any fixed primes s_1 and s_2, i.e., we should put $M = 2^k \cdot p \cdot q$ and $N = 2^k \cdot r$, where

$$p = s_1^{\alpha_1} \cdot s_2^{\beta_1} \cdot 2^{\gamma_1} - 1,\ q = s_1^{\alpha_2} \cdot s_2^{\beta_2} \cdot 2^{\gamma_2} - 1,\ r = s_1^{\alpha_3} \cdot s_2^{\beta_3} \cdot 2^{\gamma_3} - 1.$$

This leads eventually to the following result:

- *Let n and k be positive integers with $k < n$; let p, q, and r be defined as*

  $$p = (2^k - 1)2^{n-k} - 1,\ q = (2^k - 1)2^n - 1,\ r = (2^k - 1)2^{2n-k} - 1;$$

  if p, q, r are all primes, then $(M = 2^n \cdot p \cdot q, N = 2^n \cdot r)$ is an amicable pair.

This is, in fact, the Euler's rule with $k = n - x$.

Analogue of Thābit's method

4.2.11. As we have already seen, after $n = 7$, the Thābit's method, as well as the Euler's method after $n = 40$, seems to dry up and has not produced any other amicable pair.

In an effort to overcome this difficulty several authors have introduced variants of Thābit's and Euler's methods.

In 1986, Borho and Hoffmann found a new analogue of Thābit's rule for amicable pairs. The *Borho and Hoffmann's rule* gives the following algorithm:

- *Let n be a positive integer and choose x with $1 \leq x \leq n-1$ such that with $g = 2^{n-x}+1$, the number $p = 2^x \cdot g - 1$ is prime; now, choose y with $1 \leq y \leq n-1$ such that*

  $$q = 2^y + (2^{n+1}-1) \cdot g, \;\; r = 2^{n-y} \cdot g \cdot q - 1, \;\; s = 2^{n-y+x} \cdot g^2 \cdot q - 1;$$

  if q, r, s are also all primes, then $(M = 2^n \cdot q \cdot p \cdot r, N = 2^n \cdot q \cdot s)$ is an amicable pair.

☐ It is easy to check that $(p+1)(r+1) = s+1$. So, $s = pr+p+1$. Therefore,

$$\begin{aligned} M+N &= 2^n q(pr+s) = 2^n q(2s-p-r) = 2^{n+1}qs - 2^n pq - 2^n qr \\ &= 2^{n+1}qs - 2^n q(p+r) = 2^{n+1}qs - 2^n q(g(2^x + 2^{n-y}q) - 2) \\ &= 2^{n+1}qs - 2^n q(g(2^x + 2^n + 2^{n-1}(2^{n+1}g) - 2) \\ &= 2^{n+1}qs - 2^n q(g^2(2^x + 2^{n-y}(2^{n+1}-1)) - 2). \end{aligned}$$

Moreover,

$$\begin{aligned} \sigma(N) &= (2^{n+1}-1)(q+1)(s+1) = (2^{n+1}-1)(qs+q+s+1) \\ &= 2^{n+1}qs + 2^{n+1}(q+s+1) + (q+1)(s=1) \\ &= 2^{n+1}qs + (s+1)((2^{n+1}-q-1) + 2^{n+1}q) \\ &= 2^{n+1}qs + 2^n q(2^{x-y}g^2((2^{n+1}-1)(1-g) - 2^y) + 2) \\ &= 2^{n+1}qs + 2^n q(2^{x-y}g^2((2^{n+1}-1)(1-g) - 2^y) + 2) \\ &= 2^{n+1}qs + 2^n q(2^{x-y}g^2(-2^{n-x}(2^{n+1}-2^y) + 2) \\ &= 2^{n+1}qs + 2^n q(-2^{x-y}g^2(2^{n+1}-1)2^x g^2 + 2) \\ &= 2^{n+1}qs - 2^n q(2^{x-y}g^2(2^{n+1}-1)2^x g^2 - 2) \\ &= 2^{n+1}qs - 2^n q(g^2(2^x + 2^{n-y}(2^{n+1}-1)) - 2). \end{aligned}$$

So, we proved that $M+N = \sigma(N)$.

On the other hand, we have

$$\begin{aligned}\sigma(N) = \sigma(2^n qs) &= (2^{n+1}-1)(q+1)(s+1)\\ &= (2^{n+1}-1)(2^y+(2^{n+1}-1)g+1)(2^{n-y+x}g^2q),\end{aligned}$$

while

$$\begin{aligned}\sigma(M) = \sigma(2^n qpr) &= (2^{n+1}-1)(q+1)(p+1)(r+1)\\ &= (2^{n+1}-1)(2^y+(2^{n+1}-1)g+1)(2^x g)(2^{n-y}gq)\\ &= (2^{n+1}-1)(2^y+(2^{n+1}-1)g+1)(2^{n-y+x}g^2q).\end{aligned}$$

So, we proved that $\sigma(N) = \sigma(M)$.

Therefore, the condition $\sigma(M) = M + N = \sigma(N)$ holds, and the numbers $M = 2^n \cdot q \cdot p \cdot r$ and $N = 2^n \cdot q \cdot s$ form an amicable pair. □

Though this theorem was proven by Borho and Hofmann, they did not use it to find any new amicable pair. They only investigated this method for some small values of parameters and gave the example of $n = 2$, $x = 1$, $y = 1$, which corresponds to the pair

$$(M = 63020 = 2^2 \cdot 23 \cdot 5 \cdot 137, N = 76084 = 2^2 \cdot 23 \cdot 827),$$

discovered by Euler without using the theorem above.

Checking all possible parameters for $n \leq 1000$, Yan [Yan94] found that a new large amicable pair (M, N) can be obtained for $n = 47$, $x = 42$, and $y = 37$; both elements of the pair have 65 decimal digits. So,

- *for* $2 \leq n \leq 1000$, *the Borho and Hoffmann's rule generates only two amicable pairs when* $n = 2, x = 1, y = 1$ *or* $n = 47, x = 42$, $y = 37$:

$$\begin{aligned}(M,N) &= (63020, 76084);\\ (M,N) &= (2^{47} \cdot 9288811670405087 \cdot 145135534866431\\ &\quad \cdot 313887523966328699903,\\ &\quad 2^{47} \cdot 9288811670405087\\ &\quad \cdot 45556233678753109045286896851222527).\end{aligned}$$

Both these pairs as well as all five pairs obtained by Euler's rule are regular pairs of type-$(2, 1)$.

4.2.12. Of course, there are some other analogues of Thābit's and Euler's rules for amicable pairs. For example, Lee developed an algorithm for searching amicable pairs of type-$(2, 2)$. The *Lee's rule* states that

- *if, for a given positive integer n, the numbers*

  $$p = 3{\cdot}2^{n-1}-1,\ q = 35{\cdot}2^{n+1}-29,\ r = 7{\cdot}2^{n-1}-1,\ s = 15{\cdot}2^{n+1}-13$$

  are all primes, then $(M = 2^n \cdot p \cdot q, N = 2^n \cdot r \cdot s)$ is an amicable pair.

☐ It is easy to see that

$$\begin{aligned} M + N &= 2^n((3 \cdot 2^{n-1} - 1)(35 \cdot 2^{n+1} - 29) \\ &\quad + (7 \cdot 2^{n-1} - 1)(15 \cdot 2^{n+1} - 13)) \\ &= (2^{n+1} - 1)(1 - 5 \cdot 2^{2n} - 84 \cdot 2^{n-1}). \end{aligned}$$

Moreover, it holds that

$$\begin{aligned} \sigma(M) = \sigma(2^n pq) &= (2^{n+1} - 1)(p + 1)(q + 1) \\ &= (2^{n+1} - 1)(105 \cdot 2^{2n} - 84 \cdot 2^{n-1}) \\ &= (2^{n+1} - 1)(r + 1)(s + 1) = \sigma(N). \end{aligned}$$

So, $\sigma(M) = M + N = \sigma(N)$, and hence, the pair $(M = 2^n \cdot p \cdot q, N = 2^n \cdot r \cdot s)$ is an amicable pair. ☐

It can be checked that

- *for $2 \leq n \leq 5000$, the Lee's rule generates only one amicable pair when $n = 2$:*

  $$(M = 5020 = 2^2 \cdot 5 \cdot 151, N = 5564 = 2^2 \cdot 13 \cdot 107).$$

4.2.13. Experience shows that it is not easy to use pure algebraic methods such as Thābit's rule, Euler's rule, and their analogues to find new amicable pairs. More powerful methods, called *algebraic constructive methods*, are represented here by the well-known *Borho's* *rule*, which allow us to get new amicable pairs from a given "old" amicable pair, called *breeder pair* (or *mother pair*).

The algorithm of the *Boro rule* is as follows:

- *Take an amicable pair* $A = a \cdot u$, $B = a \cdot s$, *where* s *is prime, and* $(a, us) = 1$*; if* $p = u + s + 1$ *is prime and if* a *is not divisible by* p, *then check for* $n = 1, 2, 3, \ldots$ *the primality of* $q_1 = (u+1) \cdot p^n - 1$ *and* $q_2 = (u+1) \cdot (s+1) \cdot p^n - 1$*; if* q_1 *and* q_2 *are primes, then the pair* $(M = A \cdot p^n \cdot q_1, N = a \cdot p^n \cdot q_2)$ *is an amicable pair.*

□ In fact, if the numbers $A = a \cdot u$ and $B = a \cdot s$ are amicable, then $\sigma(A) = \sigma(B) = A + B$, i.e.,

$$\sigma(a)\sigma(u) = \sigma(a)(s+1) = a(u+s).$$

Therefore, it holds that

$$\frac{\sigma(a)\sigma(u)}{u+s} = \frac{\sigma(a)\sigma(u)}{p-1} = a, \ \sigma(u) = s+1,$$

and

$$\frac{\sigma(a)}{p-1} = \frac{\sigma(a)}{u+s} = \frac{a}{\sigma(u)} = \frac{a}{s+1}.$$

Then, we have

$$\begin{aligned}
\sigma(Ap^n q_1) &= \sigma(a)\sigma(u)\frac{p^{n+1}-1}{p-1}(u+1)p^n = a(u+1)p^n(p^{n+1}-1), \\
\sigma(ap^n q_2) &= \sigma(a)\frac{p^{n+1}-1}{p-1}(u+1)(s+1)p^n \\
&= \frac{a}{s+1}(p^{n+1}-1)(u+1)(s+1) \\
&= a(u+1)p^n(p^{n+1}-1), \\
Ap^n q_1 + ap^n q_2 &= p^n(au((u+1)p^n - 1) + a((u+1)(s+1)p^n - 1)) \\
&= a(u+1)p^n(up^n + (s+1)p^n - 1) \\
&= a(u+1)p^n(p^{n+1}-1).
\end{aligned}$$

So, one can state that

$$\sigma(Ap^n q_1) = \sigma(ap^n q_2) = Ap^n q_1 + ap^n q_2,$$

i.e., the numbers $A \cdot p^n \cdot q_1$ and $a \cdot p^n \cdot q_2$ form an amicable pair. □

Let us try to use the Borho's rule to find a new amicable pair from the Pythagorean pair

$$(A = 220 = 2^2 \cdot 5 \cdot 11, B = 284 = 2^2 \cdot 71).$$

As $A = 2^2 \cdot 55$ and $B = 2^2 \cdot 71$, we have that $a = 4$, $u = 55$, $s = 71 \in P$, $p = u + s + 1 = 55 + 71 + 1 = 127 \in P$, and $gcd(p, a) = 1$. So, we get the following rule (Borho called it *Thābit-rule*):

- *The pair* $(220 \cdot 127^n \cdot q_1, 4 \cdot 127^n \cdot q_2)$ *is an amicable pair for each positive integer* n *such that* $q_1 = 56 \cdot 127^n - 1$ *and* $q_2 = 56 \cdot 72 \cdot 127^n - 1$ *are both primes.*

For $n = 1$, we can see that q_1, q_2 are not primes, but for $n = 2$, we get

$$(220 \cdot 127^2 \cdot 903223, 4 \cdot 127^2 \cdot 65032127).$$

Starting from one of the Euler's pairs $(A = 3^4 \cdot 5 \cdot 11 \cdot 29 \cdot 89, B = 3^4 \cdot 5 \cdot 11 \cdot 2699)$, we have $A = 3^4 \cdot 5 \cdot 11 \cdot 2581, B = 3^4 \cdot 5 \cdot 11 \cdot 2699$, $a = 3^4 \cdot 5 \cdot 11$, and $u = 2581$. It is easy to see that $s = 2699$ and $p = u + s + 1 = 5281$ are primes.

So, we get the following rule (let it be called *Euler rule*):

- *The pair* $3^4 \cdot 5 \cdot 11 \cdot 2581 \cdot 5281^n \cdot q_1, 3^4 \cdot 5 \cdot 11 \cdot 5281^n \cdot q_2)$ *is an amicable pair for each positive integer* n *such that* $q_1 = 2582 \cdot 5281^n - 1$ *and* $q_2 = 56 \cdot 2700 \cdot 5281^n - 1$ *are both primes.*

Already for $n = 1$, we get a new amicable pair, which was found by Lee:

$$(3^4 \cdot 5 \cdot 11 \cdot 29 \cdot 89 \cdot 5281 \cdot 13635541, 3^4 \cdot 5 \cdot 115281 \cdot 36815963399),$$

te Riele proved that $n = 19$ is the next value leading to an amicable pair. However, Borho showed that there are no other values $n \leq 267$ for which this rule yields amicable pairs.

Borho's study was motivated by the question whether the set of amicable pairs of the form $(M = p^n \cdot b_1 \cdot q_1, N = p^n \cdot b_2 \cdot q_2)$ with prime p, coprime with $b_1 b_2$, can be infinite in the sense that there are infinitely many positive integers k and primes $q_1 = q_1(k), q_2 = q_2(k)$, for which the pair $(M = p^n \cdot b_1 \cdot q_1, N = p^n \cdot b_2 \cdot q_2)$ is amicable.

The theoretical base of the Borho's rule is the following fact: A necessary condition of infiniteness of the set of amicable pairs $(M = p^n \cdot b_1 \cdot q_1, N = p^n \cdot b_2 \cdot q_2)$ is the condition

$$\frac{p}{p-1} = \frac{b_1}{\sigma(b_1)} + \frac{b_2}{\sigma(b_2)}.$$

In fact, there are at least 67 (in fact, more than 2000) amicable pairs of the form $A = a \cdot u$, $B = a \cdot s$, where $s \in P$, and $(a, u \cdot s) = 1$; at least for 22 such pairs, the number $p = u + s + 1$ is prime; so, we get at least 22 new rules for generating amicable pairs.

Unfortunately, the numbers q_1 and q_2 grow very quickly with n, and very often, at least one of them is composite. Only a few amicable pairs have actually been found in this way.

Wiethaus considered a variant of Borho's rule. With the help of *Wiethaus's rule*, more than 10000 new amicable pairs were found, including the first amicable pair whose members have more than 1000 decimal digits.

For references and more information, see, for example, [Seeh84] [Dick11] [Maso21] [Poul18] [Poul48] [LeMa72], [Brow39], [Lee68], [Lee69], [BLM70], [Borh72], [AOS67], [Cohe70], [Cohe93], [Riel74], [Riel84], [Yan94], [Yan96] [Rolf65], [Rolf67], [BaBo88], [BrMc68], [GPR03], [Wiet88], [Deza17], [Cost78], [Erdo55], [Erdo76], [Esco46], [Pome77], [Pome81], and [Riel84a].

Exercises

1. The first ten amicable pairs are (220, 284), (1184, 1210), (2620, 2924), (5020, 5564), (6232, 6368), (10744, 10856), (12285, 14595), (17296, 18416), (63020, 76084), and (66928, 66992) (sequence A259180 in the OEIS). Find in this list all regular pairs. Find their types. Are there in this list any exotic pairs?

2. Find all one- and two-digit Thābit numbers $3\cdot2^n-1$. Choose from this list all primes. Choose from these primes the primes which generate an amicable pair.
3. Check that all three pairs which are obtained by the Thābit's rule are regular of the type-(2,1). What can be said about the five pairs which are obtained by Euler's rule?
4. Are all amicable pairs which we can obtain by Borho and Hoffmann's rule regular? Of which type?
5. Are amicable pairs which we can obtain by the Borho's rule (which allow us to get new amicable pairs from a given "old" amicable pair) regular?
6. Find all pairs (m, n) of positive integers such that $\tau(n) = m$ and $\tau(m) = n$.
7. What can be said about solutions to the system of equations $\sigma_2(n) = m, \sigma_2(n) = m$?

4.3. Properties of Amicable Numbers

In this section, we consider a list of well-known properties of amicable numbers.

Simplest properties of amicable pairs

4.3.1. The simplest property of amicable numbers states that

- *for any amicable pair (M, N), with $M < N$ the smaller member M is a deficient number, while the bigger member N is an abundant number.*

□ In fact, as $\sigma(M) = M + N = \sigma(N)$, and $M < N$, we get

$$\sigma(M) = M + N > M + M = 2M,\ \sigma(N) = M + N < N + N = 2N,$$

hence by definition, M is abundant and N is deficient. □

It is obvious that

- *for any amicable pair* (M, N), *the following condition holds*:

$$\frac{M}{\sigma(M)} + \frac{N}{\sigma(N)} = 1.$$

□ Recall that, by definition, for any amicable pair, it holds that

$$\sigma(M) = M + N = \sigma(N).$$

So, dividing the equality $\sigma(M) = M + N$ by $\sigma(M) = \sigma(N)$, we get

$$1 = \frac{M}{\sigma(M)} + \frac{N}{\sigma(M)} = \frac{M}{\sigma(M)} + \frac{N}{\sigma(N)}.$$

The property is proved. □

Prime factors of amicable numbers

4.3.2. It is proven that a pair of amicable numbers should have several distinct prime factors. More exactly,

- *in any amicable pair* (M, N), *one member has at least three distinct prime divisors.*

□ As an illustration, we can see that for the Thābit's and Euler's pairs, we have $M = 2^n \cdot p \cdot q$ and $N = 2^n \cdot r$, so the number N has three distinct prime factors, $2, p, q$. In general, one can obtain a contradiction using the first property in our list. For example, a pair (p, q) of two primes cannot be amicable, as both members are deficient. □

In all known amicable pairs, one member has at least two and the other has at least three different prime factors.

In general, Kanord (1953) proved that

- *if one member of the pair is of the form* p^α *and the other of the form* $q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_k^{\beta_k}$, *where* $p, q_1, q_2, \ldots, q_k$ *are distinct primes, then both members are odd,* α *is odd,* $\alpha > 1400$, $k > 300$, $N = p^\alpha > M$, *and* $M > 10^{1500}$.

Concerning amicable pairs where one member has precisely two distinct prime factors, Kanold proved also that

- *a pair* $(M = p_1^{\alpha_1} \cdot p_2^{\alpha_2}, N = q_1^{\beta_1} \cdot q_2^{\beta_2})$ *cannot be an amicable pair.*

In view of Thābit's and Euler's rules, this result is the best possible.

Borho (1974) proved that

- *if* k *is the total number of prime factors of an amicable pair* (M, N) *(counting multiple prime factors), then* $MN < k^{2^k}$.

4.3.3. Most of the smallest amicable pairs, including all pairs obtained by Thābit's and Euler's rules, are *even*, i.e., amicable pairs in which both members are even positive integers. In 1969, Lee has proved in [Lee69] that

- *neither member of an even amicable pair can contain the factor* 3.

□ Recall that, by definition, for any amicable pair, it holds that $\sigma(M) = M + N = \sigma(N)$, and so, it holds that

$$\frac{M}{\sigma(M)} + \frac{N}{\sigma(N)} = 1.$$

The deficient member N of an amicable pair $(M, N))$, $M < N$, cannot be a multiple of 3, as in this case, it is also a multiple of 6 and so should be abundant. Let M be divisible by 3. In this case,

$$M = 2^\alpha \cdot 3^\beta \cdot c,\ N = 2^\gamma \cdot b.$$

Since $N \neq 0(mod\ 3)$, we have

$$\sigma(M) = M + N = \sigma(N) \equiv 1, 2(mod\ 3).$$

So, α and γ must both be even so that $M = 2^2 \cdot 3 \cdot K$ and $N = 2^2 \cdot L$, where $K \geq 1$ and $L > 3K$ since $N > M$. For $k \geq 1$, it holds that $\frac{\sigma(M)}{M} < \frac{3}{7}$, and for $l > 3k$, it holds that $\frac{N}{\sigma(N)} < \frac{4}{7}$, a contradiction to the condition $\frac{M}{\sigma(M)} + \frac{N}{\sigma(N)} = 1$. □

4.3.4. On the other hand, it is easy to check that in many efficiently small odd amicable pairs (i.e., amicable pairs in which both members are odd), both members are divisible by 3.

Bratley and McKay (1968) conjectured that *both members of any odd pair are divisible by 3.*

This was disproved in 1988 by Borho and Battiato, who gave 15 odd amicable pairs between 10^{36} and 10^{73} with members being coprime to 6. Many more such amicable pairs were found in 1992 by Garsía. So, it is checked that

- *there are odd amicable pairs* (M, N) *such that* $gcd(M, 6) = gcd(N, 6) = 1$.

An example of such a pair with two 32-digit members is given as follows:

$$(42262694537514864075544955198125,$$
$$42405817271188606697466971841875).$$

In 1997, Kohmoto found many odd amicable pairs greater than 10^{192} with smallest prime divisor 7. In other words,

- *there are odd amicable pairs* (M, N) *such that* $gcd(M, 30) = gcd(N, 30) = 1$.

As of 2021, no odd amicable pair is coprime with 210, i.e., with smallest prime divisor greater than 7, are known.

4.3.5. In every known case, the numbers M and N of an amicable pair (M, N) are either both even or both odd. In the first case, we call such a pair an *even amicable pair*; in the second case, we call such a pair an *odd amicable pair.*

It is not known whether an *even–odd amicable pair*, i.e., an amicable pair with members of opposite parity, exists. If it does, the even member must either be a square number or twice one, and the odd number must be a square number. In other words,

- *for an even–odd amicable pair* (M, N)*, one of its members has the form* $2^{\alpha}L^2$ *and the other has the form* K^2*, where* L *and* K *are odd numbers.*

□ More precisely, Kanold (1953) proved that if $\alpha = 1$, then $M = K^2 < N = 2L^2$, and L must contained at least five distinct prime factors. If $\alpha > 1$, then $M = 2^{\alpha}L^2 < N = K^2$. □

Haggis (1970) proved that

- *for an even–odd amicable pair* (M, N)*, it holds that* $MN > 10^{121}$*, while* $M > 10^{60}$ *and* $N > 10^{60}$*.*

4.3.6. However, it is easy to check that

- *there exist amicable pairs in which the two members have different smallest prime factors.*

In fact, there are seven such pairs known.

The first example of an amicable pair where the two members have different smallest prime factors was found in 2015. It is

$$(445953248528881275 = 3^2 \cdot 5^2 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 43 \cdot 73 \cdot 439 \cdot 22483,$$

$$659008669204392325 = 5^2 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 73 \cdot 571 \cdot 1693 \cdot 5839).$$

The biggest known pair of such form is

$$(9759636606249354825 = 3^2 \cdot 5^2 \cdot 7 \cdot 11^2 \cdot 13 \cdot 139 \cdot 241 \cdot 6967 \cdot 16879,$$

$$14162430025984014775 = 5^2 \cdot 7 \cdot 11^2 \cdot 13 \cdot 223 \cdot 439 \cdot 7369 \cdot 71317).$$

4.3.7. Also, every known pair shares at least one common prime factor. It is not known whether a *relatively prime amicable pair*, i.e., an amicable pair (M, N) with coprime members M and N, exists.

It is obvious that a pair of coprime amicable numbers cannot be generated by Thābit's or Euler's rule.

However, if any such pair exists, then

- *the product* MN *of the members of a relatively prime amicable pair* (M, N) *has at least* 22 *distinct prime factors and is greater than* 10^{67}*.*

In fact, Haggis (1975) determined that

- *there are no relatively prime amicable pairs* (M, N) *with* $M < 10^{60}$.

If we fix the number of different prime factors of an amicable pair, then one can state that

- *there are only finitely many relatively prime amicable pairs with fixed number of different prime factors.*

4.3.8. Consider a pair of amicable numbers (M, N) with $M < N$; with M and N represented in the form $M = gm$, $N = gm$, where $g = gcd(M, N)$ is the greatest common divisor of M and N. If $gcd(g, m) = gcd(g, n) = 1$, and m and n are both square-free, then the pair (M, N) is said to be *regular*; otherwise, it is called *irregular* or *exotic*. If (M, N) is regular and, moreover, m and n have i and j prime factors, respectively, then (M, N) is said to be of type-(i, j).

For example, for the pair $(220, 284)$, the greatest common divisor of 220 and 284 is 4 and so $m = 55$ and $n = 71$. Therefore, (220, 284) is a regular pair of type-(2, 1).

The numbers $6955216 = 2^4 \cdot 19 \cdot 137 \cdot 167$ and $7418864 = 2^4 \cdot 463679$ form a pair of type -$(3, 1)$.

The pair $(12285 = 3^3 \cdot 5 \cdot 7 \cdot 13, 14595 = 3 \cdot 5 \cdot 7 \cdot 139)$ is exotic.

It is proven that

- *there exist no pairs of type*-$(1, j)$ *for any positive integer* $j \geq 1$.

The largest value of i for which amicable pairs of type-$(i, 1)$ are known, is $i = 7$; in 2001, Garsía found the first such amicable pair, and one year later, Pedersen found two other examples.

Sums of amicable pairs

4.3.9. In 1968, M. Gardner observed that

- *the most even pairs* (M, N) *have sums* $M + N$ *divisible by* 9.

In particular, this property holds for all Thābit's pairs. In fact, using Thābit's rule, we get that

$$\begin{aligned} M+N &= 2^n(9\cdot 2^{2n-1}-1)+2^n(3\cdot 2^{n+1}-1)(3\cdot 2^n-1) \\ &= 2^n(9\cdot 2^{2n-1}-1+9\cdot 2^{2n+1}-3\cdot 2^n \\ &\quad -3\cdot 2^{n+1}+1) = 2^n(9\cdot 2^{2n}\cdot 2{,}5-3\cdot 2^n\cdot 3) \\ &= 9\cdot 2^{2n}(5\cdot 2^{n-1}-1), \end{aligned}$$

i.e., the sum $M+N$ is divisible by 9.

However, there are even amicable pairs (M, N) with $M+N \neq 0(mod\ 9)$. For example, the amicable pair $(666030256, 696630544)$ is an amicable pair whose sum is $571750000640 \equiv 8(mod\ 9)$.

Lee (1969) noticed, in an investigation of the possible form of even amicable pairs, that only the following three pairs

$$(666030256 = 2^4\cdot 19\cdot 331\cdot 6619, 696630544 = 2^4\cdot 199\cdot 331\cdot 661),$$

$$(4150593232 = 2^4\cdot 43\cdot 61\cdot 98899, 4213181998 = 2^4\cdot 43\cdot 859\cdot 7129),$$

$$(4796703664 = 2^4\cdot 43\cdot 67\cdot 104059, 4855069456 = 2^4\cdot 43\cdot 373\cdot 18919)$$

discovered by Poulet, had sums divisible by 9.

In [Lee69], he found eight new even pairs with the same property, i.e., with the sums of pairs not divisible by 9: the first is

$$(2^4\cdot 19\cdot 6451\cdot 27103, 2^4\cdot 109\cdot 307\cdot 103231), \ldots$$

$$\ldots, (2^6\cdot 751\cdot 79\cdot 799063, 2^6\cdot 751\cdot 2239\cdot 29537).$$

In this paper, Lee characterized all the possible exceptions of the rule $M+N \equiv 0(mod\ 9)$ for even amicable pairs (M, N).

The simplest form possible for even pairs with the property

$$M+N \neq 0(mod\ 9)$$

is $(M = E\cdot p\cdot q\cdot r, N = E\cdot s)$, where p, q, r, s are distinct primes, E is even,

$$p, q, r, s \equiv 1(mod\ 6), \quad \text{and} \quad E, \sigma(E) \equiv 1(mod\ 3).$$

It was shown that there are no such simplest pairs with $E < 10^{11}$.

All the eight new pairs with sums not divisible by 9, discovered by Lee, were of the form

$$(M = E \cdot p \cdot q \cdot r, N = E \cdot p \cdot s \cdot t),$$

where p, q, r, s, t are distinct primes,

$$p, q, r, s, t, u \equiv 1(mod\ 6),\ \ E, \sigma(E) \equiv 1(mod\ 3).$$

Lee also found 121 other new pairs of the form $(M = E \cdot p \cdot q, N = E \cdot \cdot s)$ with $E < 10^5$.

Later, Pedersen listed all 557 known up to the time exceptions.

The first such pairs are

$$(666030256, 696630544), (967947856, 1031796176),$$
$$(2840437756, 3156691844),$$
$$(4150593232, 4213181968), (4796703664, 4855069456),$$
$$(10168398448, 11159012552),$$
$$(33707179456, 33844856128), (53151801712, 55270703248),$$
$$(62393407792, 65270990608), \ldots$$

(sequence A291550 in the OEIS).

4.3.10. There are also many amicable pairs (M, N) such that the sum of the pair is divisible by 10.

The first such pairs are (6232, 6368), (10744, 10856), (12285, 14595), (66928, 66992), (67095, 71145), (79750, 88730), (100485, 124155), (122265, 139815), (122368, 123152), (141664, 153176), (142310, 168730), (176272, 180848), (185368, 203432),... (sequence A291422 in the OEIS).

Considering the set of known amicable pairs, one can check that

- *more then* 80% *of amicable pairs* (M, N) *satisfy the condition* $M + N \equiv 0(mod\ 10)$.

More exactly, it is checked that up to the first 100 amicable pairs, 74% of the sums satisfy this condition; up to the first 1000: 82.5%; up to the first 2000: 85.25%; up to the first 5000: 88.1%. Among the 1947667 pairs up to 19 digits from Sergei Chernykh's database, there are 1872573 pairs with the pair sum divisible by 10, thus about 96.14%.

According to the *sum of amicable pairs conjecture*,

- *as the number of the amicable numbers approaches infinity, the percentage of the sums of the amicable pairs divisible by* 10 *approaches* 100%.

Twin amicable pairs

4.3.11. A *twin amicable pair* is an amicable pair (M, N) such that there are no integers between M and N belonging to any other amicable pair.

It is easy to check that

- *the first eight smallest amicable pairs are twin pairs.*

In fact, one can use a numerical approach to check that for the first eight amicable pairs, (220, 284), (1184, 1210), (2620, 2924), (5020, 5564), (6232, 6368), (10744, 10856), (12285, 14595), and (17296, 18416), the definition of twins holds. However, the ninth pair $(63020, 76084)$ is not a twin pair, as both the members of the next pair $(66928, 66992)$ are greater than 63020 and smaller than 76084.

The first few twin amicable pairs are (220, 284), (1184, 1210), (2620, 2924), (5020, 5564), (6232, 6368), (10744, 10856), (12285, 14595), (17296, 18416), (66928, 66992), (122368, 123152), (196724, 202444), (437456, 455344), (469028, 486178), (503056, 514736), (522405, 525915), . . . (sequence A273259 in the OEIS).

Distribution of amicable numbers

4.3.12. Let $A(x)$ be the number of amicable pairs with the smallest member of the pair not exceeding x.

For example, $A(10^3) = 1$, $A(10^4) = 5$, $A(10^5) = 13$, $A(10^6) = 42$, $A(10^7) = 108$, $A(10^8) = 236$, $A(10^9) = 586$, $A(10^{10}) = 1427$, $A(10^{11}) = 3340$, $A(10^{12}) = 7642$, $A(10^{13}) = 17519$.

In 1955, Paul Erdős showed that the density of amicable numbers, relative to the positive integers, is 0, i.e., $\lim \frac{A(x)}{x}_{x\infty} = 0$.

He improved a result by Kannold (1954) that the density of amicable pairs is less than 0.204.

His method can be used to obtain an estimate of the form $A(x) \leq \frac{cx}{\log\log\log x}$.

Erdős conjectured also that

$$A(x) = o\left(\frac{x}{(\log x)^k}\right)$$

for every k, while Pomerance (1987, 1981) proved the stronger result:

$$A(x) \leq x \cdot e^{-\sqrt[3]{\log x}}.$$

Studying the tables of amicable pairs up to 10^8–10^{10}, Bratley and te Riele conjectured that $A(x)$ is approximately proportional to $\frac{\sqrt{x}}{(\log x)^k}$, where k is some positive number.

For references and additional information, see, for example, [GPR03], [Yan96], [Borh74], [Gard68], [Garc03], [Erdo55], [Bras88], [Dick05], [Salo90], [Sier64], [Sing00], [Stru87], [Sloa22], and [Wiki22].

Exercises

1. The first 10 amicable pairs are: (220, 284), (1184, 1210), (2620, 2924), (5020, 5564), (6232, 6368), (10744, 10856), (12285, 14595), (17296, 18416), (63020, 76084), and (66928, 66992) (sequence A259180 in the OEIS). Find in this list all even pairs; all odd pairs. Are both members of each pair in the list divisible by 3?
2. Using the list of first 10 amicable pairs above, find in the list all twin amicable pairs.
3. Find the first two amicable pairs which are not twins pairs.
4. Using the list of first 10 amicable pairs above, find the sum of each pair. Are these sums divisible by 3, by 9, by 10?
5. Using the list of first 10 amicable pairs above, what can be said about prime factors of members of these pairs? Find the types of all regular pairs in the list. Check that there are no pairs with coprime members. Check that the smallest prime factors of both members in each pair from the list coincide. Check that there are no pairs of the type-$(1, j)$.

4.4. Search for Amicable Numbers

4.4.1. In the theory of perfect, amicable, and sociable numbers, there exist three classical groups of methods for finding all these three kind of special numbers. There are three essentially different types of methods of such generation, namely the exhaustive numerical searching methods, the algebraic assumption methods, and the algebraic constructive methods (for more information, see, for example, a monograph by S. Y. Yan [Yan96].

Methods of the first type are directly based on numerical calculations of values of sigma function. For example, if $\sigma(N) = \sigma(M) = N + M$, then numbers M and n form an amicable pair (M, N). On the other hand, if $\sigma(N) = 2N$, then N is a perfect number.

In the second type of methods, an assumption is made about the prime structure of the considered numbers. For example, the Thābit's rule states that for a given $n = 1, 2, 3, \ldots$, if p, q, and r are distinct primes of a special form, then the numbers $M = 2^n \cdot p \cdot q$ and $N = 2^n \cdot r$ form an amicable pair (M, N). On the other hand, for $k = 1, 2, 3, \ldots$, if $2^k - 1$ is a prime, then $N = 2^{k-1}(2^k - 1)$ is an even perfect number.

In the third type of methods, new elements of considered set of special numbers are constructed from a given (*breeder*) element of the same set. For example, the Borho's rule states that if an amicable pair $A = a \cdot u$, $B = a \cdot s$ is given, where s is prime, $(a, us) = 1$, $p = u + s + 1$ is prime, and a is not divisible by p, then the pair $(M = A \cdot p^n \cdot q_1, a \cdot p^n \cdot q_2)$ is an amicable pair for each $n = 1, 2, 3, \ldots$ such that both $q_1 = (u + 1) \cdot p^n - 1$ and $q_2 = (u + 1) \cdot (s + 1) \cdot p^n - 1$ are primes.

In this section, we present the main facts concerning the historical and contemporary aspects of the search for amicable numbers.

For this class of special numbers, all three types of searching methods are used: exhaustive numerical methods (based on the fact that $\sigma(M) = M + N = \sigma(N)$ for an amicable pair (M, N)), algebraic assumption methods (based on the Thābit's rule, its generalizations and analogue), and algebraic constructive methods (which, similar to Borho's rule, allow us to generate new amicable pairs from a given old pair).

Numerical methods for amicable pairs

4.4.2. The numerical methods are the simplest methods, in which the computation is directly based on the calculation of the sigma function; in fact, on numerical calculation of $\sigma(M)$ and $\sigma(N)$ for a checked pair (M, N) of positive integers.

Recall that a pair (m_1, m_2) is a pair of amicable numbers if

$$m_2 = \sigma(m_1) - m_1 \text{ and } m_1 = \sigma(m_2) - m_2.$$

So, we get the following simplest numerical method.

Algorithm for searching all pairs $(\boldsymbol{m_1},\boldsymbol{m_2})$ of amicable numbers with $\boldsymbol{m_1} < \boldsymbol{m_2}$, where $\boldsymbol{m_1}$ is in the interval $[\boldsymbol{A}, \mathbf{B}]$

- For m_1 from A to B, find

$$\begin{aligned} m_2 &= \sigma(m_1) - m_1 = \sigma(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) - p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s} \\ &= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+1} - 1}{p_s - 1} - p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}. \end{aligned}$$

- If $m_2 > m_1$, then find

$$\begin{aligned} m_3 &= \sigma(m_2) - m_1 = \sigma(q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \ldots \cdot q_k^{\alpha_k}) - q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \ldots \cdot q_k^{\alpha_k} \\ &= \frac{q_1^{\alpha_1+1} - 1}{q_1 - 1} \cdot \frac{q_2^{\alpha_2+1} - 1}{q_2 - 1} \cdot \ldots \cdot \frac{q_k^{\alpha_k+1} - 1}{q_k - 1} - q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \ldots \cdot q_k^{\alpha_k}. \end{aligned}$$

- If $m_3 = m_1$, then (m_1, m_2) is an amicable pair.

For $10^2 \leq m_1 \leq 10^6$, the algorithm generates 42 amicable pairs, from

$$(220 = 2^2 \cdot 5 \cdot 11, 284 = 262 \cdot 71)$$

till

$$(998104 = 2^3 \cdot 17 \cdot 41 \cdot 179, 1043096 = 2^3 \cdot 23 \cdot 5669).$$

For $10^2 \leq m_1 \leq 10^{10}$, the algorithm will generate all the 1427 amicable pairs in the range, but this would take too long to be practical.

The major computation of algorithm is the computation of $\sigma(n)$ which is based on the complete integer factorization of n. Since at the present time, no efficient factoring algorithm has been found, the algorithm cannot be performed in deterministic polynomial time.

4.4.3. In 1993, te Riele proposed a new method based on the following observation suggested by Erdős:

- *For a given positive integer s, if $x_1, x_2, \ldots, x_k, \ldots$ are integer solutions of the equation $\sigma(x) = s$, then any pair (x_i, x_j), for which $x_i + x_j = s$, is an amicable pair.*

□ The proof is obvious since, by choice of x_i and x_j, it holds that $\sigma(x_i) = x_i + x_j = \sigma(x_j) = s$. □

It is not difficult to calculate all the integers within a certain range which have the same sigma value. For example, for $200 \leq x \leq 300$, all the following integers 204, 220, 224, 246, 284, and 286 have the same sigma value of 504 but only $220 + 284 = 504$.

A critical choice of this method is the value s of the pair sum. Inspection of the pair sums of known amicable pairs revealed that in many cases, these sums only have small prime divisors. So, instead of randomly selecting the numbers as candidates for the solution of $\sigma(x) = s$, te Riele used the so-called *smooth numbers* (i.e., numbers with only small prime factors) as candidates. His idea is based on the following simple fact: If $\sigma(p^\alpha)|s$ and if $\sigma(y) = \frac{s}{\sigma(p^\alpha)}$ has a solution y with $(y, p) = 1$, then $\sigma(yp^\alpha) = \sigma(y)\sigma(p^\alpha) = s$, i.e., $x = yp^\alpha$ is a solution to the equation $\sigma(x) = s$. Based on this fact, a recursive algorithm can be designed to find a factor $\sigma(p^\alpha)$ and to solve $\sigma(y) = \frac{s}{\sigma(p^\alpha)}$ with $(y, p) = 1$. (See [Yan96] and [GPR03].)

Similar algorithms can be used for searching other classes of special numbers, defined in terms of the sigma function: *augmented amicable pairs* (m, n) with $\sigma(m) = \sigma(n) = m+n-1$, *quasi-amicable pairs* (m, n) with $\sigma(m) = \sigma(n) = m+n+1$; *multiple amicable pairs* (m, n) with $\sigma(m) = \alpha n + m$, $\sigma(n) = \beta m + n$, $\alpha \cdot \beta > 1$, *sociable k-cycles* $(m_1, m_2, \ldots, m_k)$ with $\sigma(m_1) = m_1 + m_2$, $\sigma(m_2) = m_2 + m_3, \ldots$, $\sigma(m_{k-1}) = m_{k-1} + m_k$, $\sigma(m_k) = m_k + m_1$, etc. We consider these classes of special numbers in Chapter 5.

Algebraic assumption methods for amicable numbers

In the second type of methods, an assumption is made about the prime structure of numbers m and n, which are checked as candidates for an amicable pair (m, n).

4.4.4. The *Thābit's algebraic assumption method* is based on the Thābit's rule for generating amicable pairs:

- *For a given* $n = 1, 2, 3, \ldots$, *if* $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$ *and* $r = 9 \cdot 2^{2n-1} - 1$ *are all primes, then* $(m = 2^n \cdot p \cdot q, n = 2^n \cdot r)$ *is an amicable pair.*

Although Thābit did not use his rule to find any new amicable pair beyond the Pythagorean pair $(220, 284)$, it is the first algebraic method in the theory of amicable numbers.

We present here the corresponding algorithm.

Algorithm for searching all Thābit's amicable pairs $(\mathbf{2^n} \cdot \boldsymbol{p} \cdot \boldsymbol{q}, \mathbf{2^n} \cdot \boldsymbol{r})$ with n in the interval $[\boldsymbol{A},\boldsymbol{B}]$

- For n from A to B, find

$$p = 3 \cdot 2^{n-1} - 1,\ q = 3 \cdot 2^n - 1,\ r = 9 \cdot 2^{2n-1} - 1.$$

- If p, q, r are all primes, then find

$$a = 2^n pq,\ b = 2^n r.$$

- Indicate (a, b) as an amicable pair.

From a practical point of view, to confirm the results obtained for p, q, r by probabilistic primality tests, one can use deterministic primality algorithms (such as the elliptic curve primality-proving algorithm) or apply the multiplicative property of sigma function to check where or not the following conditions hold:

$$\sigma(2^n)\sigma(p)\sigma(q) = \sigma(2^n)\sigma(r) = 2^n pq + 2^n r.$$

If p, q, r are not primes, then the above conditions cannot be satisfied.

Unfortunately, in the range $1 \le n \le 2000$, Thābit's rule only generates amicable pairs when $n = 2, 4$, and 7:

$$\begin{aligned}(220, 284) &= (2^2 \cdot 5 \cdot 11, 2^2 \cdot 71);\\ (17296, 18416) &= (2^4 \cdot 23 \cdot 47, 2^4 \cdot 1151);\\ (9363584, 9437056) &= (2^7 \cdot 191 \cdot 383, 2^7 \cdot 73727).\end{aligned}$$

Although only three amicable pairs have been generated by Thābit's rule, it is the first and one of the most important algebraic methods, and most of the modern algebraic methods are based on Thābit's ideas.

4.4.5. Based on Thābit's rule, Euler developed several new methods for generating amicable numbers and found 59 new amicable pairs.

The classical version of the *Euler's rule* states that

- *for a given positive integer* $n = 1, 2, 3, \ldots,$ *if there exists* $1 \le x \le n - 1$ *such that for* $g = 2^{n-x} + 1$*, the numbers* $p = 2^x g - 1$*,* $q = 2^n g - 1$*,* $s = 2^{n+x} g^2 - 1$ *are all primes, then* $(m = 2^n \cdot p \cdot q, n = 2^n \cdot s)$ *is an amicable pair.*

Euler's rule is a generalization of Thābit's rule. It reduces to Thābit's rule when $x = n - 1$.

We present here the corresponding algorithm.

Algorithm for searching all Euler's amicable pairs $(2^n \cdot p \cdot q, 2^n \cdot r)$ with n in the interval $[A,B]$

- For n from A to B, check all $x = 1, 2, \ldots, n - 1$.
- For a given x, find $g = 2^{n-x} + 1$; find also

$$p = 2^x g - 1, \; q = 2^n g - 1, \; s = 2^{n+x} g^2 - 1.$$

- If p, q, r are all primes, then find

$$a = 2^n pq, \; b = 2^n r.$$

- Indicate (a, b) as an amicable pair.

Similar to Thābit's method, Euler's method only gives five amicable pairs for $n \leq 1000$. The biggest pair has 40 digits in each of its members.

So, Euler's rule only gives two more pairs than Thābit's rule. No more such amicable pairs have been generated for $40 < n \leq 1000$.

However, from Euler's time, many more amicable pairs have been found, most with the help of various variations of Euler's methods.

Analogue of Thābit's method

4.4.6. In 1986, Borho and Hoffmann found a new analogue of Thābit's rule:

- *For a given positive integer* $n = 1, 2, 3, \ldots,$ *if there exists* x *with* $1 \leq x \leq n-1$ *such that for* $g = 2^{n-x} + 1$, *the number* $p = 2^x g - 1$ *is prime and then there exists* y *with* $1 \leq x \leq n-1$ *such that the numbers* $q = 2^y + (2^{n+1} - 1)g$, $r = 2^{n-y}gq - 1$, $s = 2^{n-y+x}g^2q - 1$ *are all primes, then* $(a = 2^n \cdot p \cdot q \cdot r, b = 2^n \cdot q \cdot s)$ *is an amicable pair.*

The Euler's rule is a generalization of the Thābit's rule. It reduces to the Thābit's rule when $x = n - 1$.

We present here the corresponding algorithm.

Algorithm for searching all Borho and Hoffmann's amicable pairs $(\mathbf{2}^{\boldsymbol{n}}\boldsymbol{pqr}, \mathbf{2}^{\boldsymbol{nqr}})$ with n in the interval $[\boldsymbol{A}, \boldsymbol{B}]$

- For n from A to B, check all $x = 1, 2, \ldots, n-1$.
- For a given x, find $g = 2^{n-x} + 1$; find also $p = 2^x g - 1$.
- If p is prime, then check all $y = 1, 2, \ldots, n-1$.
- For a given y, find

$$q = 2^y + (2^{n+1} - 1)g,\ r = 2^{n-y}gq - 1,\ s = 2^{n-y+x}g^2q - 1.$$

- If q, r, s are all primes, then find

$$a = 2^n pqr,\ b = 2^n qs.$$

- Indicate (a, b) as an amicable pair.

This theorem was due to Borho and Hofmann, but they did not use it to find any new amicable pair. They only investigated this method for some small values of parameters and gave the example of $n = 2$, $x = 1$, and $y = 1$, which corresponds to the pair

$$(M = 63020 = 2^2 \cdot 23 \cdot 5 \cdot 137,\ N = 76084 = 2^2 \cdot 23 \cdot 827),$$

which was discovered by Euler without using the theorem above.

Using this algorithm, Yan [Yan94] has examined all values of n, x, y with $2 \le n \le 1000$, $0 < x < n$, $0 < y < n$ and has found that $n = 47$, $x = 42$, $y = 37$ make the corresponding p, q, r, s all primes. This leads to the new amicable pair.

So, for $2 \le n \le 1000$, Borho and Hoffmann's algorithm generates only two amicable pairs when $n = 2, x = 1, y = 1$, $q = 23, p = 5, r = 137$, $s = 827$ and $n = 47, x = 42, y = 37$,

$$q = 9288811670405087,\ \ p = 145135534866431,$$

$$r = 313887523966328699903,$$

$$s = 45556233678753109045286896851222527.$$

The first pair is an Euler's pair, the second pair is a Yan's pair.

4.4.7. The *Lee's rule* states that

- *for a given positive integer* $n = 1, 2, 3, \ldots$, *if the numbers* $p = 3 \cdot 2^{n-1} - 1$, $q = 35 \cdot 2^{n+1} - 29$, $r = 7 \cdot 2^{n-1} - 1$, $s = 15 \cdot 2^{n+1} - 13$ *are all primes, then* $(a = 2^n \cdot p \cdot q, b = 2^n \cdot r \cdot s)$ *is an amicable pair.*

The corresponding algorithm is presented in the following.

Algorithm for searching all Lee's amicable pairs $(2^n pq,\ 2^n rs)$ with n in the interval $[A,\ B]$

- For n from A to B, find

$$p = 3 \cdot 2^{n-1} - 1,\ \ q = 35 \cdot 2^{n+1} - 29,\ \ r = 7 \cdot 2^{n-1} - 1,\ \ s = 15 \cdot 2^{n+1} - 13.$$

- If p, q, r, s are all primes, then find

$$a = 2^n pq,\ b = 2^n rs.$$

- Indicate (a, b) as an amicable pair.

Only one pair $(5020 = 2^2 \cdot 5 \cdot 151, 5564 = 2^2 \cdot 13 \cdot 107)$ has been found by this rule up to $n = 5000$.

Constructive methods for amicable pairs

In all these constructive methods, a given amicable pair is used as a mother pair (breeder pair) to generate new child pairs.

4.4.8. A simple constructive method for producing new amicable pairs from a given pair can be obtained using the well-known Borho's rule:

- *If an amicable pair* $X = a \cdot u$, $Y = a \cdot s$ *is given, where* s *is prime,* $(a, us) = 1$, $p = u + s + 1$ *is prime, and* a *is not divisible by* p, *then the pair* $(M = X \cdot p^n \cdot q_1, N = a \cdot p^n \cdot q_2)$ *is an amicable pair for each* $n = 1, 2, 3, \ldots$ *such that both* $q_1 = (u + 1) \cdot p^n - 1$ *and* $q_2 = (u + 1) \cdot (s + 1) \cdot p^n - 1$ *are primes.*

The corresponding algorithm is represented as follows.

Borho's algorithm for searching new amicable pairs $(M = X \cdot p^n \cdot q_1, N = a \cdot p^n \cdot q_2)$ using a given pair $(X = a \cdot \mathrm{u}, Y = a \cdot s)$ with n in the interval $[A, B]$

- Select an amicable pair $(X = a \cdot u, Y = a \cdot s)$ with prime s and $gcd(a, us) = 1$ as a mother.
- Find $p = u + s + 1$.
- If p is prime and $gcd(p, a) = 1$, then list all n from A to B.
- For a given n from A to B, find

$$q_1 = (u + 1) \cdot p^n - 1,\ q_2 = (u + 1) \cdot (s + 1) \cdot p^n - 1.$$

- If q_1, q_2 are primes, then find $M = Xp^n q_1, N = ap^n q_2$.
- Indicate (M, N) as an amicable pair.

Unfortunately, from a practical point of view, Boro's rule is not too interesting, as numbers q_1 and q_2 grow very quickly, and only few amicable pair were found using this method.

4.4.9. In 1984, Herman J. J. te Riele proposed an useful algebraic constructive method for finding new amicable pairs.

In this method, an amicable pair which is used as a breeder to generate new child pairs should necessarily be of type-$(i, 1)$ (in particular, of type-$(2, 1)$).

te Riele's rule is thus:

- *Let* $(M', N') = (a \cdot u, a \cdot p)$ *be a given amicable pair with* $gcd(a, p) = 1$*, where* p *is a prime*; *if a pair of primes* (r, s) *with* $p < r < s$ *and* $gcd(a, rs) = 1$ *exists, satisfying the bilinear Diophantine equation*

  $$(r - p)(s - p) = (p + 1)(p + u)$$

  and if a third prime q *exists with* $gcd(au, q) = 1$ *such that* $q = r + s + u$*, then* $(M = a \cdot u \cdot q, N = a \cdot r \cdot s)$ *is also an amicable pair.*

For example, choosing the amicable pair $(3^2 \cdot 5^3 \cdot 13 \cdot 59, 3^2 \cdot 5^3 \cdot 13 \cdot 18719)$, we have $a = 3^2 \cdot 5 \cdot 13$, $u = 5^2 \cdot 11 \cdot 59 = 16225$, $p = 18719$, and after factorization, we get $(p + 1)(p + u) = 2^{12}3^3 \cdot 5 \cdot 7 \cdot 13^2$. Writing $(p + 1)(p + u)$ as $2688 \cdot 243360$, we obtain the three primes $r = 18719 + 2688 = 21407$, $s = 18719 + 243360 = 262079$, and $q = 21407 + 262079 + 16225 = 299711$ and, therefore, the amicable pair

$$(3^2 \cdot 5^3 \cdot 13 \cdot 11 \cdot 59 \cdot 299711, 3^2 \cdot 5^3 \cdot 13 \cdot 21407 \cdot 262079).$$

A second amicable pair is obtained by writing $(p + 1)(p + u)$ as $3120 \cdot 20964$.

If, in addition, $gcd(a, u) = 1$, then the right-hand side of the bilinear equation above can be written as

$$(p + 1)(p + u) = \frac{\sigma(a)}{a} \cdot (\sigma(u))^2,$$

and we may expect his number to have more prime factors. So, amicable pairs of type-$(i, 1)$ with large i may be expected to be suitable as input to te Riele's rule.

The largest value of i for which amicable pairs of type-$(i, 1)$ are known is $i = 7$; in 2001, Garsía found the first such amicable pair.

The number of daughter amicable pairs, obtained with te Riele's rule from Garsía's amicable pair of type-$(7, 1)$, is 1433. The mother pair with the largest numbers of daughters, generated with te Riele's rule, namely 80136, is the pair of type-$(5, 1)$, found by Pedersen in 1997.

Consider the proof of *te Riele's rule* under the condition $gcd(a, u) = 1$. In this special case, the result can be formulated as follows.

- *Let* $(M' = a \cdot u, N' = a \cdot p)$ *be a given amicable pair with* $gcd(a, u) = gcd(a, p) = 1$*, where* p *is a prime. If a pair of primes* (r, s) *with* $p < r < s$ *and* $gcd(a, rs) = 1$ *exists, satisfying the bilinear Diophantine equation*

  $$(r - p)(s - p) = \frac{\sigma(a)}{a} \cdot (\sigma(u))^2$$

  and if a third prime q *exists with* $gcd(au, q) = 1$ *such that* $q = r + s + u$*, then* $(M = a \cdot u \cdot q, N = a \cdot r \cdot s)$ *is also an amicable pair.*

□ Since $(M', N') = (au, ap)$ is an amicable pair, we have

$$\sigma(au) = \sigma(ap),\ \sigma(u) = \sigma(p),\ \sigma(au) = \sigma(ap) = a(u + p).$$

Also, for some positive integers A and B, we can write

$$r = p + A,\ s = p + B.$$

I. If the pair (au, ap) is an amicable pair, then $\frac{\sigma(a)\sigma(u)}{a} = u + p$.

So, the condition $(r-p)(s-p) = \frac{\sigma(a)}{a} \cdot (\sigma(u))^2$ becomes $(r-p)(s-p) = (u + p)\sigma(u)$. Hence,

$$rs - p(r + s) + p^2 = (u + p)\sigma(u),\ rs - p(q - u) + p^2 = (u + p)(p + 1),$$

$$rs - p(q - u) = up + u + p,\ rs = pq + u + p.$$

Therefore, we have

$$\sigma(M) = \sigma(auq) = \sigma(apq) = \sigma(a)(p + 1)(q + 1),$$

$$\sigma(N) = \sigma(ars) = \sigma(a)(r + 1)(s + 1).$$

As $(p+1)(q+1) = pq+p+q+1 = rs-u+q+1 = rs+r+s+1 = (r + 1)(s + 1)$, then $\sigma(M) = \sigma(N)$.

II. On the other hand, it holds that

$$\begin{aligned}\sigma(M) &= \sigma(auq) = \sigma(au)\sigma(q) = a(u+p)(q+1)\\ &= a(uq+u+pq+p) = a(uq+rs),\end{aligned}$$

while

$$M+N = auq+ars = a(uq+rs).$$

This completes the proof. □

This method can be realized by the following algorithm.

te Riele's algorithm for searching new amicable pairs using a given pair

- Select a type-$(i,1)$ amicable pair (M', N') as a breeder.
- Rewrite the breeder pair as (au, ap) in order to get a, u, and p.
- Compute $R = \frac{\sigma(a)}{a} \cdot (\sigma(u))^2$.
- Factor R into its prime decomposition form: $R = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$.
- Generate all the possible combinations $R = A \cdot B$, $A < B$.
- Test all such combinations by computing and primary testing of r, s, q:

$$r = p + A,\ \ s = p + B,\ \ q = r + s + u.$$

- If r, s, q are all primes, $gcd(a, rs) = 1$, and $gcd(au, q) = 1$, then find $M = auq, N = ars$.
- Indicate (M, N) as an amicable pair.

For example, consider as a breeder pair the 65-digit pair, found by Yan in 1994 (see [Yan94]). So, we get a pair (au, ap) with

$$a = 2^{47} \cdot 9288811670405087,$$

$$u = 145135534866431 \cdot 313887523966328699903,$$

$$p = 45556233678753109045286896851222527.$$

In this case,

$$\begin{aligned}R = \frac{\sigma(a)}{a} \cdot (\sigma(u))^2 &= 2^{62}3^7 \cdot 5 \cdot 7 \cdot 11^4 \cdot 13 \cdot 17 \cdot 97 \cdot 214 \cdot 257 \cdot 673\\ &\cdot 96758454900053 \cdot 9288811670405087.\end{aligned}$$

It is easy to see that R is a 70-digit integer with 1249280 even divisors less than its square root, each having even co-divisor. With these combinations, R is written in all possible ways as a product

$$R = A \cdot B$$

such that

$$r = p + A,\ \ s = p + B,\ \ q = r + s + u.$$

If r, s, q are primes, $r < s$, $gcd(a, rs) = 1$, then $(M = a \cdot u \cdot q, a \cdot r \cdot s)$ is an amicable pair.

Testing all the possible 1249280 combinations of $R = A \cdot B$, 95 new amicable pairs have been found from Yan's 65-digit mother pair.

Moreover, using this rule, te Riele has completed a search for all daughter pairs from the known 234 type-$(i, 1)$ breeder pairs. He found 13122 daughter pairs including the 95 pairs represented above.

4.4.10. In 1968, Lee proposed a general algebraic method for constructing amicable pairs. It was based on the obvious fact that any amicable pair can be written in the form $(M = a_1 \cdot p \cdot q, N = a_2 \cdot r)$, where $gcd(a_1, p) = gcd(a_1, q) = gcd(a_2, r) = 1$.

For given a_1, a_2, Lee's method allows us to find all possible values of p, q, r by using all possible decompositions $X \cdot Y$ of the value $\sigma(a_2)(a_1a_2\sigma(a_2) + \sigma(a_1)(a_1 - a_2)(a_1 - \sigma(a_2)))$.

Unfortunately, it is very difficult to find a_1, a_2 such that p, q, r are integral, and Lee's method is essentially impractical.

Yan [Yan96] proposed another general method for constructing amicable pairs. His algorithm, starting from a breeder pair $(M', N') = (a_1p, a_2q)$, uses the given numbers a_1, a_2 to calculate a constant $W = W(a_1, a_2)$. After complete factorization of W into its prime decomposition form, one should consider all possible decompositions $W = UV, U < V$. For each combination $W = UV, U < V$, the numbers $q_1 = q_1(U, a_1, a_2)$, $q_2 = q_2(V, a_1, a_2)$, $p_1 = p_1(q_1, q_2, a_1, a_2)$ should be calculated. If q_1, q_2, p_1 are all primes (and hence integers), then under some additional conditions ($q_1 \neq q_2$, $gcd(a_2, q_1q_2) = 1$, $gcd(a_1, p_1) = 1$), one obtains a new amicable pair

$$(M = a_1 \cdot p_1, N = a_2 \cdot q_1 \cdot q_2).$$

This method is general, as any amicable pair, including exotic, could be used as breeder pairs to construct new (usually large) amicable pairs.

There exist two other general constructive methods also based on the representation of an amicable pair (M, N) in the form $(M, N) = (wm, wn)$, where $w = gcd(M, N)$ and $gcd(w, m) = gcd(w, n) = 1$.

The *forward methods* start from a common factor w of M and N and try to find two other factors m and n such that $(M, N) = (wm, wn)$ is an amicable pair.

The *backward methods* start with two given factors m and n of M and N and try to find a number w such that $(M, N) = (wm, wn)$ is an amicable pair. In this case, the numbers w, m, n are not necessarily primes.

For detailed consideration of these methods as well as most of the algorithms presented in this section, one can refer to [Yan96]. For an additional information see, for example, [BoHo86], [Lee68] [Riel84], [Deza17], and [Wiki22].

Exercises

1. Using Borho's rule and starting from Pythagorean amicable pair (220, 284), construct a new amicable pair (it is, for example, $(220 \cdot 127^2 \cdot 903223, 4 \cdot 127^2 \cdot 65032127)$).
2. Using Borho's rule and starting from Euler's amicable pair, $(3^4 \cdot 5 \cdot 11 \cdot 29 \cdot 89$ and $3^4 \cdot 5 \cdot 11 \cdot 2699)$, construct a new amicable pair (it is, for example, $(3^4 \cdot 5 \cdot 11 \cdot 29 \cdot 89 \cdot 5281 \cdot 13635541, 3^4 \cdot 5 \cdot 115281 \cdot 36815963399)$).
3. Check that any Thābit number can be represented as $2^{n-1}+2^n-1$.

4.5. Amicable Numbers in the Family of Special Numbers

Amicable numbers as deficient and abundant numbers

4.5.1. In this section, we consider natural connections between amicable, deficient, and abundant numbers. Recall that numbers with the sum of their proper divisors less than the number itself are called *deficient* and where it is greater than the number, *abundant.*

The first few deficient numbers are 1, 2, 3, 4, 5, 7, 8, 9, 10, 11,... (sequence A005100 in the OEIS), while the first abundant numbers are 12, 18, 20, 24, 30, 36, 40, 42, 48, 54,... (sequence A005101 in the OEIS).

In Chapter 3, we provided a list of simple properties of deficient and abundant numbers:

- All prime numbers are deficient.
- All prime powers p^k, $k \in \mathbb{N}$, are deficient.
- The product of two primes except $2 \cdot 3$ is deficient.
- All odd numbers with one or two distinct prime factors are deficient.
- Any divisor of a deficient number is deficient.
- Any $n = 2 \cdot 3^k$, $k > 1$, is abundant.
- Every multiple of a perfect number (except the perfect number itself) is abundant.
- Every multiple of an abundant number is abundant.

In Section 4.3, we proved that

- *in any amicable pair, the bigger member is deficient and the smaller member is abundant.*

As in an amicable pair (M, N), the numbers M and N cannot be simultaneously deficient and abundant, we can state that:

- there exists no amicable pair (p, q) with two prime members;
- there exists no amicable pair (p^k, q^s), $p, q \in P, k, s \in \mathbb{N}$, in which both members are powers of primes;
- there exists no amicable pair in which both members are products of two primes;
- there exists no amicable pair in which both members have at most two distinct prime factors;
- there exists no amicable pair in which both members are divisible by 6.

4.5.2. Moreover, using the functions $s(n)$ and $\sigma(n)$, we can define other classes of special numbers relative to amicable numbers: augmented amicable pairs (m, n) with $\sigma(m) = \sigma(n) = m + n - 1$, quasi-amicable pairs (m, n) with $\sigma(m) = \sigma(n) = m + n + 1$; multiple amicable pairs (m, n) with $\sigma(m) = \alpha n + m$, $\sigma(n) = \beta m + n$, $\alpha \cdot \beta > 1$, sociable k-cycles $(m_1, m_2, \dots, m_k)$ with $\sigma(m_1) = m_1 + m_2$, $\sigma(m_2) = m_2 + m_3, \dots$, $\sigma(m_{k-1}) = m_{k-1} + m_k$, $\sigma(m_k) = m_k + m_1$, etc. We consider these classes of special numbers in Chapter 5.

Amicable numbers and aspiring numbers

4.5.3. There exists one more class of special numbers closely connected with the notion of divisor functions and, hence, with the theory of perfect and amicable numbers.

Let

$$s(n) = \sum_{d|n,\ d\neq n} d = \sigma(n) - n$$

be the *restricted divisor function*, and we define the *aliquot sequence of* n as

$$s^0(n) = n, s^1(n) = s(n), s^2(n) = s(s(n)), \dots, s^k(n) = s(s^{k-1}(n)), \dots.$$

Many aliquot sequences terminate at 0, all such sequences necessarily end with a prime number followed by 1 (since the only proper divisor of a prime is 1), followed by 0 (since 1 has no proper divisors).

The first numbers whose aliquot sequence terminates with 1 are 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16,... (sequence A080907 in the OEIS).

All primes are in this set because $s(p) = 1$ for any prime p.

However, there are a variety of ways in which an aliquot sequence might not terminate.

A *perfect number* N forms the constant aliquot sequence $N, N, N, \dots$, i.e., has a repeating aliquot sequence of period 1. For example, the aliquot sequence of 6 is 6, 6, 6, 6, ...

An *amicable number* (e.g., the number M from an amicable pair (M, N)) forms the aliquot sequence $M, N, M, N, \dots$, i.e., has a repeating aliquot sequence of period 2. For instance, the aliquot sequence of 220 is 220, 284, 220, 284, . . . , while the aliquot sequence of 284 is 284, 220, 284, 220, ...

A *sociable number* has a repeating aliquot sequence of period 3 or greater. For instance, the aliquot sequence of 1264460 is 1264460, 1547860, 1727636, 1305184, 1264460, ...

Some numbers have an aliquot sequence which is eventually periodic, but the number itself is not perfect, amicable, or sociable. For instance, the aliquot sequence of 95 is 95, 25, 6, 6, 6, 6, ... Numbers such as 95 that are not perfect but have an eventually repeating aliquot sequence of period 1 are called *aspiring numbers*.

In other words, an *aspiring number* is a positive integer that is not perfect but whose aliquot sequence becomes constant after a finite numbers of steps. The first few aspiring numbers are 25, 95, 119, 143, 417, 445, 565, 608, 650, 652, 675, 685, 783, 790, 909, . . . (sequence A063769 in the OEIS).

There are many numbers whose aliquot sequences have not yet been completely computed, so this sequence is not fully known. In particular, 276 may, perhaps, be an element of this sequence, although this is very unlikely.

Numbers less than 1000 with unknown aliquot sequences are 276, 306, 396, 552, 564, 660, 696, 780, 828, 888, 966, and 996.

The following list indicates the termination number of the aliquot sequence starting at $n = 1, 2, 3, \ldots$: 1, 2, 3, 3, 5, 6, 7, 7, 3, 7, 11, 3, 13, 7, 3, . . . (sequence A115350 in the OEIS). Here, $a(n)$ gives the prime number if the sequence terminates in a prime followed by 1 (as an exception, $a(1) = 1$), $a(n)$ gives a perfect number if the sequence terminates in a perfect number (check that in the list there exists no number that terminates at 28, the second perfect number!), $a(n)$ gives the smallest number of the cycle if the sequence terminates in an aliquot cycle, $a(n) = 0$ if the sequence is open ended. So far, 276 is the smallest number for which the termination of the aliquot sequence is not known.

Catalan's conjecture states that *every aliquot sequence terminates in a prime number followed by* 1*, a perfect number, a friendly pair, or an aliquot cycle.*

Amicable numbers and prime numbers

4.5.4. In the context of Thābit's, Euler's, and other rules, which allow us to generate amicable pairs, we are interested in prime numbers which take part in formulas of such type.

The simplest algebraic formula which produces amicable pairs is Thābit's formula:

- *If* $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$, *and* $r = 9 \cdot 2^{2n-1} - 1$ *are all primes, then* $(M = 2^n \cdot p \cdot q, n = 2^n \cdot r)$ *is an amicable pair.*

Numbers of the form $3 \cdot 2^n - 1$ are known as *Thābit numbers*.

Formally, a *Thābit number* (or *Thābit ibn Qurra number*, or *321 number*) is an integer of the form $3 \cdot 2^n - 1$ for a non-negative integer n.

The first few Thābit numbers are 2, 5, 11, 23, 47, 95, 191, 383, 767, 1535, 3071, 6143, 12287, 24575, 49151,. . . (sequence A055010 in the OEIS).

The first few Thābit numbers that are prime (*Thābit primes* or *321 primes*) are 2, 5, 11, 23, 47, 191, 383, 6143, 786431, 51539607551, 824633720831,. . . (sequence A007505 in the OEIS).

As of 2021, there are 64 known prime Thābit numbers. Their n-values are 0, 1, 2, 3, 4, 6, 7, 11, 18, 34, 38, 43, 55, 64, 76,. . . . 2312734, 3136255, 4235414, 6090515, 11484018, 11731850, 11895718, 16819291, 17748034 (sequence A002235 in the OEIS).

The primes for $234760 \leq n \leq 3136255$ were found by the distributed computing project *321 search*.

In 2008, *PrimeGrid* took over the search for Thābit primes. It is still searching and has already found all currently known Thābit primes with $n \geq 4235414$.

4.5.5. When both n and $n-1$ yield Thābit primes, and $9 \cdot 2^{2n-1} - 1$ is also prime, a pair of amicable numbers can be calculated by well-known algorithms.

For example, $n = 2$ gives the Thābit prime 11, $n-1 = 1$ gives the Thābit prime 5, and our third term is 71. Then, $2^2 = 4$, multiplied by 5 and 11 results in 220, whose divisors add up to 284, and 4 times 71 is 284, whose divisors add up to 220.

The only known n satisfying these conditions are 2, 4, and 7, corresponding to the Thābit primes 11, 47, and 383 given by n, the Thābit primes 5, 23, and 191 given by $n-1$, and the third prime terms 71, 1151, and 73727. The corresponding amicable pairs are (220, 284), (17296, 18416), and (9363584, 9437056).

It is easy to check that

- *the binary representation of the Thābit number* $3 \cdot 2^n - 1$ *is* $n+2$ *digits long, consisting of "10" followed by* n *ones.*

For example, $5 = 101_2$, $11 = 1011_2$, $23 = 10111_2$, etc.

□ In fact, $3 \cdot 2^n - 1 = 2^{n+1} + (2^n - 1) = 2^{n+1} + 2^{n-1} + 2^{n-2} + \cdots + 2 + 1 = 1011\ldots11_2$. □

4.5.6. The *PrimeGrid* project is also searching for primes of the form $3 \cdot 2^n + 1$, such primes are called *Thābit primes of the second kind* (or *321 primes of the second kind*).

The first few Thābit numbers of the second kind are 4, 7, 13, 25, 49, 97, 193, 385, 769, 1537, 3073, 6145, 12289, 24577, 49153,... (sequence A181565 in the OEIS).

From them, the first few *Thābit primes of the second kind* are 7, 13, 97, 193, 769, 12289, 786433, 3221225473, 206158430209, 6597069766657, 221360928884514619393,... (sequence A039687 in the OEIS).

Their n values are 1, 2, 5, 6, 8, 12, 18, 30, 36, 41, 66, 189, 201, 209, 276,... (sequence A002253 in the OEIS).

4.5.7. For integer $b \geq 2$, a *Thābit number base* b is defined as a number of the form $(b+1) \cdot b^n - 1$ for a non-negative integer n.

Similarly, for integer $b \geq 2$, a *Thābit number of the second kind base* b is a number of the form $(b+1) \cdot b^n + 1$ for a non-negative integer n.

The *Williams numbers* are also a generalization of Thābit numbers. For integer $b \geq 2$, a *Williams number base* b is a number of the form $(b-1) \cdot b^n - 1$ for a non-negative integer n, as well as a *Williams number of the second kind base* b is a number of the form $(b-1) \cdot b^n + 1$ for a non-negative integer n.

Ordinarily, a *Thābit prime base b* is a Thābit number base b that is prime, and a *Williams prime base b* is a Williams number base b that is also prime. It is easy to check that

- *every prime p is a Thābit prime of the first kind base p, a Williams prime of the first kind base $p+2$, and a Williams prime of the second kind base p; if $p \geq 5$, then p is also a Thābit prime of the second kind base $p-2$.*

There exists a conjecture that

- *for every integer $b \geq 2$, there are infinitely many Thābit primes of the first kind base b, infinitely many Williams primes of the first kind base b, and infinitely many Williams primes of the second kind base b.*

Moreover, it is conjectured that

- *for every integer $b \geq 2$, $b \neq 1 (mod\ 3)$, there are infinitely many Thābit primes of the second kind base b.*

If the base b is congruent to 1 modulo 3, then all Thābit numbers of the second kind base b are divisible by 3 and greater than 3, so

- *there are no Thābit primes of the second kind base b.*

4.5.8. *Pierpont numbers* $3^m \cdot 2^n + 1$ are a generalization of Thābit numbers of the second kind, $3 \cdot 2^n + 1$.

Gauss proved that we can subdivide a circle into n parts using a ruler (an unmarked straightedge) and a compass (which draws circles) if and only if n is a power of two times a product of distinct *Fermat primes.*

Later, Pierpont proved (1895) that we can divide a circle into n parts using origami (paper folding) if and only if n is a product of a power of two times a power of three times a product of distinct primes of the form $2^u \cdot 3^v + 1$, $u, v \geq 0$, i.e., times a product of distinct *Pierpont primes.*

The first few Pierpont primes are 2, 3, 5, 7, 13, 17, 19, 37, 73, 97, ... (sequence A005109 in the OEIS).

As any Fermat prime is a Pierpont prime $2^u \cdot 3^v + 1$ (with $v = 0$, $u = 2^n$), then any constructible polygon can be constructed using origami.

On the other hand, a *Pierpont prime of the second kind* is a prime number of the form $2^u 3^v - 1$, $u, v \geq 0$.

So, any Thābit's prime is a Pierpont prime of the second kind $2^u 3^v - 1$ with $v = 1$, while any Mersenne prime is a Pierpont prime of the second kind $2^u 3^v - 1$ with $v = 0$.

Moreover, the third prime $9 \cdot 2^{2n-1} - 1$ from the Thābit's rule is also a Pierpont prime of the second kind $2^u 3^v - 1$ with $v = 2$ and an odd u.

These numbers are 2, 3, 5, 7, 11, 17, 23, 31, 47, 53, 71, 107, 127, 191, 383, ... (sequence A005105 in the OEIS).

The largest known primes of this type are Mersenne primes; currently, the largest known is $2^{82589933} - 1$. The largest known Pierpont prime of the second kind that is not a Mersenne prime, it is $3 \cdot 2^{11895718} - 1$, so a Thābit's prime. It was found by *PrimeGrid*.

Amicable numbers and Gaussian integers

4.5.9. Amicable pairs are two integers where the sum of the proper divisors of one is the other and vice versa.

Since the Gaussian integers have many of the properties of the regular integers, we sought to discover whether there exist any pairs of Gaussian integers with the same property.

For the definition of *Gaussian amicable numbers*, we should consider the ring $(\mathbb{Z}[i], +, \cdot)$ of *Gaussian integers*,

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}, \quad \text{where } i^2 = -1,$$

and try to construct the sum of divisors function $\sigma_{\mathbb{Z}[i]}(a + bi)$ for this ring.

Having $\sigma_{\mathbb{Z}[i]}(a + bi)$, one can define a *Gaussian amicable pair* as a pair (M, N), $M, N \in \mathbb{Z}[i]$, such that it holds that

$$\sigma_{\mathbb{Z}[i]}(M) = M + N = \sigma_{\mathbb{Z}[i]}(N).$$

In the case of acceptable choice, one can obtain for Gaussian perfect numbers an analogue of Thābit's rule. (see, for example, [Spir18] and [McDa74]).

In fact, in [Clar13], it is shown that the pair

$$(736 - 16560i = (1+i)^8 \cdot (45+2i) \cdot 23 \cdot (-i),$$
$$17648 + 768i = (1+i)^8(1103+48i))$$

is a Gaussian amicable pair as well as the ordinary amicable pair

$$\begin{aligned}&(294706414233, 305961592167)\\&\quad = (3^4 \cdot 7^2 \cdot 11 \cdot 19 \cdot 47 \cdot 7559, 3^4 \cdot 7 \cdot 11 \cdot 19 \cdot 971 \cdot 2659),\end{aligned}$$

discovered by te Riele in 1995.

However, the smallest ordinary amicable pair $(220, 284)$ (as well as any ordinary amicable pair of type-$(2,1)$ is not a Gaussian amicable pair in the interpretation by Clark (2013), [Clar13].

It is possible also to use a similar approach for the construction of *Eisenstein amicable numbers* in the ring $(\mathbb{Z}[\omega], +, \cdot)$ of *Eisenstein integers*,

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}, \quad \text{where } \omega = \frac{-1+i\sqrt{3}}{2}.$$

For more information about the construction of the sum of divisors function $\sigma_{\mathbb{Z}[\omega]}(a+b\omega)$ in the ring $(\mathbb{Z}[\omega], +, \cdot)$ of Eisenstein integers and the choice an analog of classical condition $\sigma(M) = M + N = \sigma(N)$ for ordinary (rational) amicable numbers (M, N), which allows us to obtain Eisenstein amicable numbers an analogue of Thābit ibn Qurra theorem, see, for example, [Smal02].

For some additional information, see, for example, [Buch09], [Deza17], [Deza21], [Wiki22], [Sloa22], [Dick05], [Pier95], [Weis22], and [Prim22].

Exercises

1. Prove that there are no amicable pairs of the form (p^α, q^β), $p, q \in P$; $(p_1 p_2, q_1 q_2)$, $p_i, q_j \in P$; $(6m, 6n)$, $m, n \in \mathbb{N}$.

2. Find the first 10 Thābit numbers; choose from this list all primes. How many Thābit primes lead to an amicable pair? What can be said about binary representation of Thābit numbers? Prove that, with the exception of 5, no Thābit number is palindromic in binary.
3. Find the first 10 Thābit numbers of the second kind; choose from this list all primes. What can be said about the binary representation of Thābit numbers of the second kind?
4. Check that 25, 95, 119, and 143 are aspiring numbers, i.e., their aliquot sequences terminate by a perfect number.
5. Find the terminated number of the aliquot sequence starting at $n = 1, 2, 3, \ldots, 30$. How many sequences are terminated by $(p, 1)$, where $p \in P$? Why the term p before 1 is a prime? How many sequences are terminated by $a, a, a, \ldots$? Why the number a is perfect?
6. A Pierpont number is a positive integer of the form $3^u 2^v + 1$. Find the first 10 Pierpont numbers; first 10 Pierpont primes. Prove that any Fermat number is a Pierpont number.
7. A Pierpont number of the second kind is a positive integer of the form $3^u 2^v - 1$. Find the first 10 Pierpont numbers of the second kind; first 10 Pierpont primes of the second kind. Prove that any Thābit number is a Pierpont number of the second kind. Prove that any Mersenne number is a Pierpont number of the second kind. Prove that all three primes from the Thābit's rule are Pierpont primes of the second kind.

4.6. Open Problems

In the theory of amicable numbers, there are several well-known open problems, among which the biggest one is the following:

- Are there infinitely many amicable pairs?

4.6.1. In order to discuss this open question and other questions and conjectures of the theory of amicable numbers, let us recall some basic definitions of this theory.

An amicable pair (M, N) is called an *even amicable pair* if it is in the form

$$(M = 2^{\alpha} \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},\ N = 2^{\beta} \cdot q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r}),$$

where 2 is the smallest prime factor in both M and N.

The smallest amicable pair $(220 = 2^2 \cdot 5 \cdot 11, 284 = 2^2 \cdot 71)$ is obviously even. An example of a sufficiently big even amicable pair is as follows:

$$(1699746184 = 2^2 \cdot 23 \cdot 41 \cdot 233 \cdot 967,\ 1725115256 = 2^3 \cdot 17 \cdot 12684671).$$

An amicable pair (M, N) is called an *odd amicable pair* if it is in the form

$$M = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},\ N = q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r},$$

where the smallest prime factors p_1, q_1 in both M and N are odd.

The smallest odd amicable pair is the seventh amicable pair

$$(12285 = 3^3 \cdot 5 \cdot 7 \cdot 13, 14595 = 3 \cdot 5 \cdot 7 \cdot 139);$$

the next two are

$$(67095 = 3^3 \cdot 5 \cdot 71, 71145 = 3^3 \cdot 5 \cdot 17 \cdot 31)$$

and

$$(69615 = 3^2 \cdot 7 \cdot 13 \cdot 5 \cdot 17, 87633 = 3^2 \cdot 7 \cdot 13 \cdot 107).$$

An amicable pair (M, N) is called an *even–odd amicable pair* if it is in the form

$$M = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},\ N = q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r},$$

where one of the smallest prime factors p_1, q_1 of M and N is even (e.g., equals 2) and other is odd.

There are no known pairs of such form.

An amicable pair (M, N) is called a *relatively prime amicable pair* if M and N are coprime, i.e., if the pair has the form

$$M = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},\ N = q_1^{\beta_1} \ldots q_r^{\beta_r},$$

where all $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_r$ in both M and N are distinct prime numbers.

As before, there are no known pairs of such form.

An amicable pair (M, N), $M < N$, is called a *regular amicable pair* if M and N can be represented in the form $M = gm$, $N = gn$, where $g = gcd(M, N)$ is the greatest common divisor of M and N, m, n are both square-free, and $gcd(g, m) = gcd(g, n) = 1$. Otherwise, the pair M, N is called *irregular* (or *exotic*). If (M, N) is regular and, moreover, if m and n have i and j as prime factors, respectively, then (M, N) is said to be of *type*-(i, j).

For example, the pair $(220, 284)$ is a regular pair of type-(2, 1). The numbers

$$(6955216 = 2^4 \cdot 19 \cdot 137 \cdot 167,\ 7418864 = 2^4 \cdot 463679)$$

form a pair of type-$(3, 1)$. The pair $(12285 = 3^3 \cdot 5 \cdot 7 \cdot 13, 14595 = 3 \cdot 5 \cdot 7 \cdot 139)$ is exotic.

For a given amicable pair (M, N), the number $M + N$ is called the *pair sum* (or *sum of pair*). For any known amicable pair (i.e., even or odd), its pair sum is an even number having some special characteristics. For example, for many amicable pairs, their pair sums are divisible by 10, while a lot of pairs have pair sums divisible by 9.

All pairs from the examples above share these properties. Obviously, all five pair sums are divisible by 10; moreover,

$$220 + 884 = 504 = 9 \cdot 46,$$

$$1699746184 + 1725115256 = 3424861440 = 9 \cdot 380540160.$$

4.6.2. The answer to the main question of the theory of amicable numbers, *Are there infinitely many amicable pairs?* is, probably, "yes."

Though Erdős proved that

- *the density of the set of amicable pairs, relative to the positive integers, is* 0*, i.e.,*

$$\lim \frac{A(x)}{x}_{x \to \infty} = 0,$$

where $A(x)$ is the number of amicable pairs with the smallest member of the pair not exceeding x, today (2021) there are over 1227267785 known amicable pairs.

Numerical analysis of the tables of amicable pairs up to 10^{10} and theoretical arguments allow us to conjecture that

- *the value* $A(x)$ *is approximately proportional to* $\frac{\sqrt{x}}{(\log x)^k}$ *with some positive* $k \geq 1$.

The relative conjectures deal with perfect numbers (as a particular case of amicable numbers, see Chapter 3) and with sociable numbers (as a generalization of amicable numbers, see Chapter 5). In fact, the following conjectures are well known in number theory:

- There are infinitely many amicable pairs.
- There are infinitely many perfect numbers.
- There are infinitely many sociable numbers.

4.6.3. Similar questions can be formulated about some subclasses of amicable numbers.

- "Are there infinitely many even amicable pairs?"
- "Are there infinitely many odd amicable pairs?"
- "Are there infinitely many even–odd amicable pairs? Moreover, does there exists at least one even–odd amicable pair?"
- "Are there infinitely many relative prime amicable pairs? Moreover, does there exists at least one relative prime amicable pair?"

The answer to the first two questions probably should be "yes."

As for the last two questions, if there exist even–odd or relative prime amicable pairs, they should be very special and very big.

However, from Euler's time, we have the two well-known conjectures:

- *There exists at least one amicable pair with opposite parity.*
- *There exists at least one amicable pair* (M, N) *with gcd*$(M, N) = 1$.

Euler was probably the first to consider the above two conjectures.

No answer has been found yet. It seems to be as hard and inaccessible as the existence of odd perfect numbers.

However, if one changes the conjecture "There exists at least one amicable pair with opposite parity," taking instead of the condition "exactly one member of a pair is divisible by 2" the similar condition "exactly one member of a pair is divisible by 3," one obtains the following proposition, which is still a conjecture in the theory of amicable numbers:

- *There exists at least one odd amicable pair* (M, N) *with* N *but not* M *(or with* M *but not* N*) divisible by* 3.

This problem seems to be tractable with today's technologies.

4.6.4. The "divisibility by 3"-property is an important part of many propositions about amicable numbers. It is well known that both members M and N of any even amicable pair (M, N) are not divisible by 3, e.g., $gcd(M, 3) = gcd(N, 3) = 1$. However, before 1988, all known odd amicable pairs were of the form

$$N = 3^n \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},\ M = 3^n \cdot q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r},$$

so 3 was the smallest odd prime factor in both M and N.

Thus, Bratley and Mckay in 1968 conjectured that *all odd amicable pairs must be divisible by 3.*

This was shown to be false by Battiato and Borho in 1988. They found 15 counterexamples which are not divisible by 3. All these 15 new odd amicable pairs were of the form

$$N = 5^n \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},\ M = 5^n \cdot q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r},$$

so the smallest odd prime factor in both M and N was 5.

An example of such a pair with two 32-digit members is given as follows:

$$(42262694537514864075544955198125,$$
$$42405817271188606697466971841875).$$

In 1997, Kohmoto found many odd amicable pairs greater than 10^{192} with the smallest prime divisor 7.

However, while at present, over 1000 pairs coprime to $30 = 2 \cdot 3 \cdot 5$ are known (Kohmoto, 1997; García, Pedersen, and te Riele, 2003; Sándor and Crstici, 2004; etc.), the problem of finding amicable pairs coprime to $210 = 2 \cdot 3 \cdot 5 \cdot 7$ is still open. So, we have the following conjecture:

- *There exist amicable pairs* (M, N) *such that every prime factor of* M *and* N *is at least* 11.

4.6.5. The conjecture above is a part of one much more general conjecture which states that

- *given a prime* p, *there is an amicable pair* (M, N) *such that every prime factor of* M *and* N *is at least* p.

At present, all known amicable pairs either have $p = 2, 3, 5$, or 7. None are known with $p > 7$.

Since there are infinitely many primes, the last conjecture implies that the main amicable pairs' conjecture "There are infinitely many amicable pairs."

One more very general question is:

- *Are there regular amicable pairs of all possible types?*

4.6.6. There are two famous results connected with pair sums $M + N$.

It is obvious that *the most known even pairs* (M, N) *have pair sums* $M + N$ *divisible by 9.*

In particular, it holds that for all pairs generated by using the Thābit's rule

$$\begin{aligned} M + N &= 2^n(9 \cdot 2^{2n-1} - 1) + 2^n(3 \cdot 2^{n+1} - 1)(3 \cdot 2^n - 1) \\ &= 2^n(9 \cdot 2^{2n-1} - 1 + 9 \cdot 2^{2n+1} - 3 \cdot 2^n - 3 \cdot 2^{n+1} + 1) \\ &= 2^n(9 \cdot 2^{2n} \cdot 2,5 - 3 \cdot 2^n \cdot 3) = 9 \cdot 2^{2n}(5 \cdot 2^{n-1} - 1). \end{aligned}$$

However, there are even amicable pairs (M, N) with $M + N \neq 0(mod\ 9)$. For example, the amicable pair $(666030256, 696630544)$ is a pair whose sum is $571750000640 \equiv 8(mod\ 9)$.

In 1969, Lee [Lee69] found several such pairs in the list of the known amicable pairs and constructed eight new even pairs with the same property.

In this paper, Lee characterized also all the possible exceptions of the rule $M + N \equiv 0(mod\ 9)$ for even amicable pairs (M, N).

In all, 557 exceptions of the pair sums $M + N$ are equal to 2 or to 0 modulo 3.

So, an open question is:

- *Does there exists an amicable pair with pair sum equal to* 1 *modulo* 3*?*

There are also many amicable pairs (M, N) such that the sum of the pair is divisible by 10.

It is checked that up to the first 5000 amicable pairs, 88.1% of the sums satisfy this condition.

According to the *sum of amicable pairs conjecture*,

- *as the number of the amicable numbers approaches infinity, the percentage of the sums of the amicable pairs divisible by* 10 *approaches* 100%*.*

4.6.7. Finally, consider some conjectures related to prime numbers considered in the theory of amicable numbers.

Recall that the prime numbers of the form $3 \cdot 2^n - 1$, $n \geq 0$, are known as *Thābit primes*.

They are sufficiently used in the Thābit's formula: In order for Ibn Qurra's formula to produce an amicable pair, two Thābit primes for consecutive indexes $n - 1, n$ must be obtained.

As of 2021, there are 64 known prime Thābit numbers. The smallest is 2, the biggest known is $3 \cdot 2^{17748034} - 1$. So, at present, we do not know

- *if there are infinitely many Thābit primes.*

A *Pierpont prime of the second kind* is defined as a prime number of the form $2^u 3^v - 1$, $u, v \geq 0$.

So, any Thābit's prime is a Pierpont prime of the second kind $2^u 3^v - 1$ with $v = 1$, while any Mersenne prime is a Pierpont prime of the second kind $2^u 3^v - 1$ with $v = 0$. Moreover, the third prime $9 \cdot 2^{2n-1} - 1$ from Thābit's rule is also a Pierpont prime of the second kind $2^u 3^v - 1$ with $v = 2$ and an odd u.

The largest known primes of this type are Mersenne primes; currently, the largest known is $2^{82589933} - 1$. The largest known Pierpont prime of the second kind that is not a Mersenne prime is $3 \cdot 2^{11895718} - 1$, so a Thābit's prime. It was found by *PrimeGrid*.

The open question of the form:

- "*Are there infinitely many Pierpont primes of the second kind?*"

leads us to the famous *Mersenne conjecture* about infiniteness of the set of Mersenne primes.

On the other hand, the *Pierpont primes of the first kind*, defined as prime numbers of the form $2^u 3^v + 1$, $u, v \geq 0$, give for $v = 0$ the set of Fermat primes. It is another example of interesting mathematical facts connected with the theory of amicable pairs.

There are other sets of primes of special form which can be listed in connection with our consideration.

For integer $b \geq 2$, a *Thābit prime base b* is defined as a prime of the form $(b+1) \cdot b^n - 1$ for a non-negative integer n. Similarly, for integer $b \geq 2$, a *Thābit prime of the second kind base b* is a number of the form $(b+1) \cdot b^n + 1$ for a non-negative integer n.

For integer $b \geq 2$, a *Williams prime base b* is a prime of the form $(b-1) \cdot b^n - 1$ for a non-negative integer n, as well as a *Williams prime of the second kind base b* is a prime of the form $(b-1) \cdot b^n + 1$ for a non-negative integer n.

There is a conjecture that

- *for every integer $b \geq 2$, there are infinitely many Thābit primes of the first kind base b, infinitely many Williams primes of the first kind base b, and infinitely many Williams primes of the second kind base b.*

If the base b is congruent to 1 modulo 3, then all numbers of the form $(b+1) \cdot b^n + 1$ are divisible by 3. However, there is a conjecture that

- *for every integer $b \geq 2$, $b \neq 1 (mod\ 3)$, there are infinitely many Thābit primes of the second kind base b.*

For some additional information, see, for example, [Dick05], [GPR03], [Yan96], [Deza17], [Deza21], [BrMc68], and [BaBo88].

Exercises

1. The first 10 amicable pairs are (220, 284), (1184, 1210), (2620, 2924), (5020, 5564), (6232, 6368), (10744, 10856), (12285, 14595), (17296, 18416), (63020, 76084), and (66928, 66992) (sequence A259180 in the OEIS). Check that for all these pairs, the pair sums equal 0 or 2 modulo 3. Check that it is true for all amicable pairs represented in this chapter.
2. Using the list of the first 10 amicable pairs above, check that for any amicable pair in the list, both members have common prime factor $p \in \{2, 3, 5, 7\}$. Check that it is true for all amicable pairs represented in this chapter.
3. Prove that if the *Mersenne conjecture* "There are infinitely many Mersenne primes" is true, then the conjecture "There are infinitely many Pierpont primes of the second kind" is true.
4. Prove that if the conjecture "There are infinitely many Pierpont primes" is false, then the conjecture "The number of Fermat primes is finite" is true.

References

[AbSt72], [IrRo90], [AGP94], [Andr98], [Arno38], [Apos86], [Avan67], [BaCo87], [Buch09], [Cohn65], [CoGu96], [CoRo96], [Dede63], [DeDe12], [DeKo13], [Deza17], [Deza18], [Dick05], [Diop74], [ErOb37], [Eule48], [Gard61], [Gard88], [Gees20], [GKP94], [Guy94], [HaWr79], [John77], [Ingh32], [Ivic85], [Kara83], [Lagr70], [Land09], [Lege79], [LiNi96], [LiNi96], [Luca75], [Mada79], [MSC96], [Moze09], [Nage51], [Ore48], [Hogg69], [Pasc54], [Plut78], [RaTo57], [SlPl95], [Smit84], [Gard88], [Kobl87], [Kobl87], [Shan93], [Sier64], [Vile14], [Weis22], [Well86], and [Wiki22].

This page intentionally left blank

Chapter 5

Generalizations and Analogue

5.1. History of the Question

5.1.1. The history of generalizations of perfect and amicable numbers is quite new.

First of all, this is the history of sociable numbers. Mathematicians count it from 1918, when Pulet found the two first aliquot cycles.

However, as sociable numbers are a generalization of perfect and amicable numbers, we can consider the long and rich history of these two famous classes of numbers as a part of the history of sociable numbers. Then, it stars from Pythagorean time (see Chapters 3 and 4).

On the other hand, there are other generalizations and analogues of classical case, such as multiply perfect, quasi-perfect, almost perfect numbers, amicable k-tuples, etc. Some of these numbers were known a long time ago.

For example, an *untouchable number* is a positive integer that cannot be expressed as the sum of all the proper divisors of any positive integer (including the untouchable number itself). That is, these numbers are not in the image of the aliquot sum function $s(n)$. Their study goes back at least to Abu Mansur al-Baghdadi (circa AD 1000), who observed that both 2 and 5 are untouchable.

5.1.2. *Sociable numbers* are numbers whose aliquot sums form a cyclic sequence that begins and ends with the same number. They are generalizations of the concepts of amicable numbers and perfect numbers.

More precisely, in an aliquot sequence, each number is the sum of the proper factors of the preceding number, i.e., the sum excludes the preceding number itself. Starting at n, we get the sequence $n, s(n), s(s(n)), s(s(s(n))), \ldots$, where $s(n) = \sum_{d|n,\ d \neq n} d$. For the sequence to be sociable, the sequence must be cyclic and return to its starting point.

The period of the sequence or order of the set of sociable numbers is the number of elements in this cycle.

If the period of the sequence is 1, the number is a sociable number of order 1 or is a perfect number. A pair of amicable numbers is a set of sociable numbers of order 2.

In general, if the period is $k \geq 3$, the number is called *sociable of order k*. For example, 1264460 is a sociable number of order 4 since its aliquot sequence is $1264460, 1547860, 1727636, 1305184, 1264460, \ldots$.

There are no known sociable numbers of order 3, although searches for them have been made up to $5 \cdot 10^7$ as of 1970 and up to $5 \cdot 10^{12}$ as of 2021.

The smallest members of sociable quadruples are 1264460, 2115324, 2784580, 4938136, 7169104, 18048976, 18656380, 28158165, 46722700, 81128632,... (sequence A090615 in the On-Line Encyclopedia of Integer Sequences, OEIS). The largest known 4-cycle has 71 digits. Up to $5 \cdot 10^{12}$, the listing for aliquot-4-cycles is exhaustive.

There are many sociable numbers of order 4 and several known sociable numbers of order $k \geq 5$ (see the following table).

The first two sociable sequences or sociable chains, namely the sets of orders 5 and 28, were discovered and named by the Belgian mathematician Paul Poulet (1887–1946) in 1918. W. Borho constructed one of length 4 in 1969. H. Cohen was the first to use a computer to find nine new 4-aliquot cycles in 1970.

The first few sociable numbers are 112496, 14316, 1264460, 2115324, 2784580, 4938136, 7169104, 18048976, 18656380, 28158165,

... (sequence A003416 in the OEIS), which have orders 5, 28, 4, 4, 4, 4, 4, 4, 4, 4,..., respectively (sequence A052470 in the OEIS). The following table (see [Wiki22]) summarizes the smallest members of known social cycles as well as the number of such cycles known.

Excluding perfect numbers, a total of 152 sociable cycles were known as of 2009; more than 5000 are known as of 2021 (see tables by D. Moews, J. O. M. Pedersen, S. Chernykh, W. Creyaufmüller, Ch. Clavier, and others).

k	OEIS	Number of known cycles	Smallest k-sociable number
4	A090615	5398	1264460
5	A072891	1	12496
6	A119478	5	21548919483
8		4	1095447416
9		1	805984760
28	A072890	1	14316

5.1.3. It is an open question whether all aliquot sequences end up at either a sociable number or at a prime (and hence 1) or, equivalently, whether there exist numbers whose aliquot sequence never terminates and hence grows without bound.

This question about the possible behavior of aliquot sequences was first published by the Belgian mathematician Eugène Catalan in 1888. In 1913, Leonard Eugene Dickson extended it to the so-called *Catalan's conjecture*: "Each aliquot sequence ends in a prime, in a perfect number or in an aliquot cycle."

Up to now, it has not been possible to certify the Catalan's conjecture.

Normally, an aliquot sequence ends in a prime. Different sequences can come together and end in the same prime. All these side sequences are called a *prime family.* New calculations occasionally lead to a confluence of two former different aliquot sequences into one family.

Each confluence of two sequences gives some more hope, but it's no proof of the conjecture, it's only progress toward a possible solution. A great step in this direction was taken in 2005 by C. Clavier; he found the confluence of sequences 1578 and 56440 with a record descent.

It is possible that there are quite small numbers missing from the sequence $12496, 14316, 1264460, 2115324, 2784580, 4938136, \ldots$ (sequence A003416 in the OEIS) of all sociable numbers. There is no proof that 564 (for example) is missing (or not). Starting at 564, the aliquot sequence continues for at least 3486 steps, reaching a 198-digit number after 3486 iterations. Although it seems unlikely, there is no way to be completely certain that the forward aliquot sequence doesn't meet the backwards tree; if it did, 564 would be part of a (very long) aliquot cycle.

Many other numbers are (or were) in a similar situation.

The smallest *start-up number* (or *key number* or *beginning number*) n for which there was ever a doubt was 138, but Lehmer showed that the sequence terminates at $s^{177}(138) = 1$. Since then, the first number whose behavior is not known, i.e., the start-up number of such a so-called *open-ended sequence*, is 276. Many researchers have investigated the behavior of this sequence, but it is not yet known if its end exists.

There are five open-ended sequences in the interval [1, 1000] with the key numbers 276, 552, 564, 660, and 966. They are called *Lehmer five*.

Before the year 1980, there were 14 main sequences starting between 1000 and 2000 (*Godwin fourteen*), but at the present time, only 12 remain unknown. Godwin showed that the 1848 sequence terminates and so did Dickerman for the 1248 one.

In 1994, A. W. P. Guy and R. K. Guy published an article with a table showing the status of the sequences starting with numbers less than or equal to 7044. In the same year, the book *Unsolved problems in Number Theory* (2nd ed.), by R. K. Guy, updates the information of the article. In this book, an extensive bibliography on this subject can be found.

Since then, M. Benito and J. L. Varona have been checking the aliquot sequences for numbers under 10000. For some starting values, they have shown for the first time that the sequence terminates.

In 1996, they found the record for the maximum of a terminating sequence: The one starting at 4170 converges to 1 after 869 iterations getting a maximum of 84 decimal digits at iteration 289.

In 1999, W. Bosma found that the aliquot sequence starting with 44922 terminates at 1 after 1,689 iterations and reaches a maximum of 85 digits at step 1167. A bit later in 1999, he showed that the sequence starting at 43230 finished: It terminates at 1 after 4,357 steps and reaches a maximum of 91 digits at step 967.

In 2001, M. Benito and J. L. Varona had proved that the sequence starting at 3630 reaches a maximum of 100 digits at index 1263 and ends at 1 at step 2624 (with the prime 59 being the previous term). Later in 2001, they found that the sequence starting at 6160 finished: It terminates at 1 after 3,027 steps (with the prime 601 being the previous term) after reaching a maximum of 96 digits at step 1631.

At present, there are 81 open-ended sequences in the interval $[1, 10^4]$; 898 open-ended sequences in the interval $[1, 10^5]$; and 9190 open-ended sequences in the interval $[1, 10^6]$. Any progress in calculation can reduce these numbers.

5.1.4. By substituting some other functions relative to $s(n)$, we can construct various other classes of special numbers. For example, if we set $s^+(n) = s(n) + 1$, the fixed points of $s^+(n)$ are called *almost perfect numbers* (or *augmented perfect numbers*). All powers of 2 are almost perfect; no other almost perfect numbers are known. The 2-cycles of $s^+(n)$ have been called *augmented amicable pairs*, and we can define *augmented sociable numbers* similarly. There exists a list of 188 augmented amicable pairs with smaller members less than 10^9 (D. Moews).

Similarly, if we set $s^-(n) = s(n) - 1$, we get *quasi-perfect numbers* (or *reduced perfect numbers*), *quasi-amicable*, (or *reduced amicable*) *numbers* (also called *betrothed numbers* because each number in the pair is the sum of the proper divisors, greater than 1, of the other) and *reduced sociable numbers*. Quasi-perfect numbers must be odd squares above 10^{35}; none are known. There exists a list of the 180 pairs of reduced amicable numbers below 10^9 (D. Moews).

One can generalize all these notions in various ways by changing the criterion we use to say when one number divides another.

To generalize the notion of divisibility, we can consider, for example, *unitary, bi-unitary, infinitary, and exponential divisors* of n.

After making corresponding definitions, we can talk about *unitary* (*bi-unitary, infinitary*, etc.) *perfect, amicable*, and *sociable numbers*, as well as about *reduced* (*augmented*, etc.), *unitary* (*bi-unitary, infinitary*, etc.) *perfect, amicable*, and *sociable numbers*.

The most interesting question about these generalizations is *whether there exists an infinite number of unitary perfect numbers.* At present, just five are known.

There exists a list of all generalized aliquot cycles, defined as above, with members preceding the largest member less than $2 \cdot 10^{11}$ (D. Moews).

5.1.5. A similar, but more general, approach was proposed by Y. Kohmoto. He considered a generalization of the sociable numbers defined according to the generalized aliquot sequence

$$a(n) = \frac{\sigma(a(n-1))}{m}, \ m \in \mathbb{N}.$$

Multiply perfect numbers are fixed points of this mapping since if $a(n) = a(n-1)$, then

$$ma(n) = \sigma(a(n)),$$

which is the definition of an m-perfect number. If the sequence $a(n)$ becomes cyclic after $k > 1$ terms, it is then called a $\frac{1}{m}$-*sociable number of order* k.

An example of $\frac{1}{2}$-sociable numbers of order 2 can be constructed using Mersenne primes. In fact, if M_p, M_q are two distinct Mersenne primes, then the numbers $2^{m-1}M_n$ and $2^{n-1}M_m$ form a $\frac{1}{2}$-sociable pair.

For references and many additional information, see, for example, [Poul18], [Well86], [Cohe70], [Cohe93], [Guy94], [MoMo91], [MoMo93], [Borh69], [Cata88], [Dick13], [BLM70], [HaCo82], [Wall72], [Wall75], [StSu74], [Dick05], [Yan96], [Sloa22], [Weis22], and [Wiki22]. Many interesting facts can also be found on the Internet: See, for example, the webpages of D. Moews, J. O. M. Pedersen, S. Chernykh, W. Creyaufmüller, Ch. Clavier, and others.

5.2. Relatives of Perfect Numbers

Semiperfect numbers

5.2.1. A *semiperfect number* (or *pseudoperfect number*) is a natural number that is equal to the sum of all or some of its proper divisors.

For example, the number 12 is semiperfect, as it has proper divisors 1, 2, 3, 4, and 6, and $2+4+6=12$; the number 20 is semiperfect, as it has proper divisors 1, 2, 4, 5, and 10, and $20=1+4+5+10$. On the other hand, the number 4 is not semiperfect, as it cannot be represented as a sum of its proper divisors 1 and 2.

The first few semiperfect numbers are 6, 12, 18, 20, 24, 28, 30, 36, 40, 42, 48, 54, 56, 60, 66,... (sequence A005835 in the OEIS).

A semiperfect number that is equal to the sum of all its proper divisors is a perfect number. So,

- *any perfect number is semiperfect.*

Following the definition, we obtain that

- *any semiperfect number is necessarily either perfect or abundant.*

□ In fact, for a semiperfect number n, it holds that

$$\sigma(n) = n + \sum_{d|n, d<n} d \geq n + n = 2n, \quad \text{and} \quad \sigma(n) \geq 2n.$$

In the case of equality, we get a perfect number; in the case of inequality, we get an abundant number. □

It is easy to check that

- *every multiple of a semiperfect number is semiperfect.*

□ In fact, if n is equal to the sum of its proper divisors $d_1, \ldots, d_m$, then any of its multiple kn, $k \in \mathbb{N}$, is equal to the sum of its proper divisors $kd_1, \ldots, kd_m$ and hence is semiperfect. □

From the last property, it holds that

- *there are infinitely many semiperfect numbers.*

□ For example, any number of the form $6t, t \in \mathbb{N}$, is semiperfect. □

As 945 is semiperfect (it is the smallest odd semiperfect number), then, moreover,

- *there are infinitely many odd semiperfect numbers.*

An algorithm for the construction of new semiperfect numbers is represented as follows:

- *If k is a positive integer and p is a prime such that $2^{k-1} < p < 2^{k+1}$, then $2^k p$ is semiperfect.*

□ In fact, the divisors of this number are

$$1, 2, \ldots, 2^k, p, 2p, \ldots, 2^k p.$$

As $p < 2^{k+1}$, then in the base 2, we have

$$p = c_{k-1} \cdot 2^{k-1} + \cdots + c_1 \cdot 2 + c_0, \ c_i \in \{0, 1\}.$$

Therefore,

$$\begin{aligned} 2^k p = (2^k - 1)p + p = (1 + 2 + \cdots + 2^{k-1})p + p = p + 2p \\ + \cdots + 2^{k-1}p + c_0 + c_1 \cdot 2 + \cdots + c_{k-1} \cdot 2^k \end{aligned}$$

is the needed sum representation of $2^k p$. □

In particular, we can state that

- *every number of the form $2^k(2^{k+1} - 1)$ is semiperfect (indeed, perfect, if $2^{k+1} - 1$ is a Mersenne prime).*

There are some classes of special numbers which are semiperfect.

5.2.2. Recall that a *practical number* is a positive integer n such that all smaller positive integers can be represented as sums of distinct divisors of n. One can prove that

- *every practical number that is not a power of two is semiperfect.*

□ In fact, any power of two is abundant and so cannot be semiperfect. On the other hand, for any practical number n which has an odd prime divisor p, if all numbers $1, 2, \ldots, n-1$ are represented as sums of distinct divisors of n, then n itself has a similar representation. See Chapter 4 for more explanations. □

5.2.3. A *primary pseudoperfect number* is a positive integer n satisfying the *Egyptian fraction equation*

$$\frac{1}{n} + \sum_{p \mid n} \frac{1}{p} = 1,$$

where the sum is over only the prime divisors of n.

It is obvious that

- *each primary pseudoperfect number except* 2 *is also semiperfect.*

□ Using the definition above, we obtain that for a primary semiperfect number n, the following representation holds:

$$1 + \sum_{p \mid n} \frac{n}{p} = n.$$

Except for the primary semiperfect number 2, this expression gives a representation for n as the sum of distinct divisors of n. So, n is semiperfect. □

The eight known primary pseudoperfect numbers are 2, 6, 42, 1806, 47058, 2214502422, 52495396602, and 84904215835596884107067712 61086 (sequence A054377 in the OEIS).

5.2.4. We can see that there are sufficiently many semiperfect numbers. In fact, it is proven (Erdős) that

- *the density of the set of semiperfect numbers exists.*

5.2.5. A semiperfect number that is not divisible by any smaller semiperfect number is called *primitive semiperfect number* (or *primitive pseudoperfect number* or *irreducible semiperfect number* or *irreducible pseudoperfect number*).

It follows from the list of the semiperfect numbers that, for example, the numbers 6 and 20 are primitive semiperfect while the numbers $12 = 6 \cdot 2$ and $18 = 6 \cdot 3$ are not primitive semiperfect.

The first few primitive semiperfect numbers are 6, 20, 28, 88, 104, 272, 304, 350, 368, 464, 490, 496, 550, 572, 650,... (sequence A006036 in the OEIS).

It is proven that

- *there are infinitely many primitive semiperfect numbers.*

□ In fact, any number of the form $2^k p$, where k is a positive integer and p is a prime such that $2^{k-1} < p < 2^{k+1}$ is primitive semiperfect. □

However, there are primitive semiperfect numbers of other forms, e.g., 770. Moreover, it is proven that

- *there are infinitely many odd primitive semiperfect numbers as well as infinitely many primitive semiperfect numbers that are not harmonic divisor numbers.*

5.2.6. A *weird number* is a positive integer that is abundant but not semiperfect.

The smallest weird number is 70. Its proper divisors are 1, 2, 5, 7, 10, 14, and 35; these sum to 74, but no subset of these sums to 70.

The first few weird numbers are 70, 836, 4030, 5830, 7192, 7912, 9272, 10430, 10570, 10792, 10990, 11410, 11690, 12110, 12530,... (sequence A006037 in the OEIS).

It is easy to show that

- *if n is weird and p is a prime greater than $\sigma(n)$, then pn is also weird.*

□ In fact, in this case, the decomposition of pn as a sum of its distinct divisors implies the corresponding decomposition of n; a contradiction. It is proven in [BeEr74] using an investigation of the function $\frac{\sigma(n)}{n}$. □

It allow us to state that

- *there are infinitely many weird numbers.*

□ For example, $70p$ is weird for all primes $p \geq 149$. □

In fact, it is proven in [BeEr74] that

- *the set of weird numbers has positive density.*

All known weird numbers are even. It is not known *if any odd weird numbers exist.* If so, they must be greater than 10^{21}. Moreover,

- *any even weird number must have at least three distinct prime factors.*

□ This is true since all numbers of the form $2^k \cdot p^m$ are deficient or semiperfect (in particular, perfect, if $m = 1$ and $p = 2^{k+1} - 1$ is a Mersenne prime). □

5.2.7. Similar to primitive semiperfect numbers, a *primitive weird number* is defined as a weird number that is not a multiple of other weird numbers.

Of course, the first weird number 70 is primitive as well as the next five weird numbers. The first weird number which is a non-primitive weird number is $10430 = 70 \cdot 149$. In fact, the first few primitive weird numbers are 70, 836, 4030, 5830, 7192, 7912, 9272, 10792, 17272, 45356, 73616, 83312, 91388, 113072, 243892,... (sequence A002975 in the OEIS).

Benkovski and Erdős [BeEr74] found all the weird numbers less than 10^6. In the following table, all primitive weird numbers up to 10^4 are given, and the description of all non-primitive weird numbers less than 10^6 is represented.

Primitive weird	Non-primitive weird
70	$70p, p > \sigma(70) = 144, p \in P$
836	$7192 \cdot 31$
4030	$836 \cdot 421$
5830	$836 \cdot 487$
7192	$836 \cdot 491$
7912	$836 \cdot p, p > 557, p \in P$
9272	

There are only 24 primitive weird numbers smaller than a million, the smallest being 70 and the biggest 786208, compared to 1765 weird numbers up to that limit.

It is conjectured that

- *there exist infinitely many primitive weird numbers.*

At present, primitive weird numbers with as many as 16 prime factors and 14712 digits have been found.

Melfi (2015) has shown that the infiniteness of primitive weird numbers is a consequence of *Cramér's conjecture*, which gives an estimate for the size of gaps between consecutive prime numbers: Intuitively, the gaps between consecutive primes are always small, and the conjecture states that $p_{n+1} - p_n = O((\log p_n)^2)$, where p_n denotes the nth prime number.

Kravitz (1976) has shown that

- *for a positive integer k, if p is a prime exceeding 2^k such that the number $q = \frac{2^k p-(p+1)}{(p+1)-2^k}$ is also prime and greater than 2^k, then $n = 2^{k-1}pq$ is a weird number.*

With this formula, he found the large weird number

$$n = 2^{56} \cdot (2^{61} - 1) \cdot 153722867280912929 \;\approx\; 2 \cdot 10^{52}.$$

The construction by Kravitz yields primitive weird numbers since all weird numbers of the form $2^k pq$ are primitive, but the existence of infinitely many k and p which yield a prime q is not guaranteed. So, this construction cannot be used for the proof of infiniteness of the set of weird numbers.

5.2.8. An *untouchable number* is a positive integer that cannot be expressed as the sum of all the proper divisors of any positive integer (including the untouchable number itself). That is, these numbers are not in the image of the aliquot sum function $s(n)$.

Their study goes back at least to Abu Mansur al-Baghdadi (circa AD 1000), who observed that

- *both 2 and 5 are untouchable.*

In fact, the number 2 is untouchable, as it cannot be represented as a sum of two distinct positive integers; so, it is not the sum of the proper divisors of any positive integer. The number 5 is untouchable, as the sum $5 = 1+4$ is the only way to write 5 as the sum of distinct positive integers including 1, but if 4 divides a number, 2 does also, so 1 + 4 cannot be the sum of all of any number's proper divisors since the list of factors would have to contain both 4 and 2. On the other hand, the number 4 is not untouchable, as it is equal to the sum of the all proper divisors of 9: $1+3=4$.

The first few untouchable numbers are: 2, 5, 52, 88, 96, 120, 124, 146, 162, 188, 206, 210, 216, 238, 246,... (sequence A005114 in the OEIS).

It is conjectured that

- *the number* 5 *is the only odd untouchable number.*

□ This proposition, which has not been proven, would follow from a slightly stronger version of the *Goldbach conjecture.*

In fact, the sum of the proper divisors of the product pq of two distinct primes p and q is $1+p+q$. Thus, *if a number* n *can be written as a sum of two distinct primes, then* $n+1$ *is not an untouchable number.*

It is expected that *every even number larger than 6 is a sum of two distinct primes*; so, probably, no odd number larger than 7 is an untouchable number. In addition, $1=\sigma(2)-2$, $3=\sigma(4)-4=1+2$, $7=\sigma(8)-8=1+2+4$, so only 5 can be an odd untouchable number. □

Thus, it appears that

- *besides* 2 *and* 5*, all untouchable numbers are composite numbers.*

□ Really, except 2, all even numbers are composite. □

As, by definition, any perfect number can be expressed as the sum of its own proper divisors, we get that

- *no perfect number is untouchable.*

Similarly,

- *none of the amicable numbers are untouchable.*

Also,

- *all Mersenne numbers are not untouchable.*

□ In fact, any number $M_n = 2^n - 1$ can be expressed as the sum $1 + 2 + \cdots + 2^{n-1}$ of proper divisors of 2^n. □

It is easy to see that

- *no untouchable number is one more than a prime number.*

□ Really, any number $p + 1$ with prime p can be represented as the sum of the proper divisors 1 and p of p^2; it is $p + 1$. □

Also, one can check that

- *no untouchable number is three more than a prime number, except* 5.

□ In this case, any number $p+3$ with odd prime p can be represented as the sum of the proper divisors $1, 2, p$ of $2p$; it is $p + 3$. □

According to Erdős (1973),

- *there are infinitely many untouchable numbers.*

Moreover, according to Chen and Zhao (2011),

- *the density of the set of untouchable numbers is at least* 0.06.

5.2.9. One more class of special numbers, closely connected with divisor function, are the so-called *Erdős–Nicolas numbers*: positive integers that are not perfect but that equals one of the partial sums of their divisors.

That is, a number n is an Erdős–Nicolas number if there exists another number m such that

$$\sum_{d|n,\ d\leq m} d = n.$$

For example, the number 24 is an Erdős–Nicolas number since $24 = 1 + 2 + 3 + 4 + 6 + 8$, where $1 < 2 < 3 < 4 < 6 < 8$ are consecutive divisors of 24.

The first few Erdős–Nicolas numbers are 24, 2016, 8190, 42336, 45864, 392448, 714240, 1571328, 61900800, 91963648, 211891200, 1931236608, 2013143040, 4428914688, 10200236032, . . . (sequence A194472 in the OEIS).

They are named after Paul Erdős and Jean-Louis Nicolas, who wrote about them in 1975.

Multiply perfect numbers

5.2.10. Given $k \in \mathbb{N}$, a positive integer n is called *k-perfect* (or *k-fold perfect*) if the sum of all positive divisors of n is equal to kn:

$$\sigma(n) = kn.$$

A number that is k-perfect for a certain k is called a *multiply perfect number* (or *multiple perfect number* or *multiperfect number* or *pluperfect number*).

For example, the number 6 is 2-perfect since

$$\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6;$$

the number 120 is 3-perfect:

$$\sigma(120) = \sigma(2^3 \cdot 3 \cdot 5) = 15 \cdot 4 \cdot 6 = 3 \cdot 120.$$

The only 1-perfect number is 1. In fact,

- 1 *is the only known odd multiply perfect number.*

By definition,

- *any perfect number is multiply perfect number; in fact, it is* 2-*perfect.*

The set of multiply perfect numbers starts from 1, 6, 28, 120, 496, 672, 8128, 30240, 32760, 523776, 2178540, 23569920, 33550336, 45532800, 142990848, ... (sequence A007691 in the OEIS).

5.2.11. As of 2021, k-perfect numbers are known for each value of k up to 11.

The number 120 is the first 3-perfect number. The next few 3-perfect (or *triperfect*) numbers are $672, 523776, 459818240, 1476304896, 51001180160, \ldots$ (see sequence A005820 in the OEIS).

There are only six known 3-perfect numbers, and they are believed to comprise all such numbers.

The first few 4-perfect numbers are

$$30240,\ 32760,\ 2178540,\ 23569920,\ 45532800,\ 142990848,$$
$$1379454720,\ 43861478400,\ 66433720320,\ 153003540480,$$
$$403031236608,\ 704575228896,\ 181742883469056,$$
$$6088728021160320,\ 14942123276641920, \ldots$$

(sequence A005820 in the OEIS). It is conjectured (Sloane, 2012) that there are only finitely many terms in this sequence.

All known 5-perfect numbers are

$$14182439040,\ 31998395520,\ 518666803200,\ 13661860101120,$$
$$30823866178560,\ 740344994887680,\ 796928461056000,$$
$$212517062615531520,\ 69357059049509038080,$$
$$87934476737668055040,\ 170206605192656148480$$

(sequence A005820 in the OEIS). It is conjectured that this sequence is finite; moreover, probably, these are its only terms.

All known 6-multiperfect numbers are represented as follows:

$$154345556085770649600,\ 9186050031556349952000,$$
$$680489641226538823680000,\ 6205958672455589512937472000,$$
$$13297004660164711617331200000,\ 15229814702070563916152832000$$

(sequence A046061 in the OEIS). Similar to 5-perfect numbers, it is conjectured that this sequence is finite and probably has exactly six (already known) elements.

As of 2021, there are exactly 5772 multiply perfect numbers.

The first k-perfect numbers for $k = 1, 2, 3, \ldots$ are given by the sequence

$$1,\ 6,\ 120,\ 30240,\ 14182439040,\ 154345556085770649600,$$
$$141310897947438348259849402738485523264343544818565120000, \ldots$$

(sequence A007539 in the OEIS).

There exists a hypothesis that *all* k*-perfect numbers with* $k = 3, 4, 5, 6,$ *and* 7 *are found.*

5.2.12. There are several interesting properties of multiply perfect numbers. For example,

- *if there exists an odd perfect number* m*, then* $2m$ *would be* 3*-perfect.*

□ In fact, it holds since $\sigma(2m) = \sigma(2) \cdot \sigma(m) = 3 \cdot (2m)$. □

However, there is no known odd perfect number as well as no odd 3-perfect number. But, similar to odd perfect (i.e., 2-perfect) numbers, it is proven that

- *an odd* 3*-perfect number must be a square number exceeding* 10^{70} *and have at least* 12 *distinct prime factors, the largest exceeding* 10^5*.*

It is easy to show also that

- *the product of any two coprime perfect numbers is a* 4*-perfect number.*

□ In fact, if n and m are perfect and $gcd(n, m) = 1$, then $\sigma(mn) = \sigma(n)\sigma(m) = (2n) \cdot (2m) = 4 \cdot (mn)$. □

So, an odd perfect number (unlikely to exist) and infinitely many Mersenne primes will make the sequence of 4-perfect numbers infinite. However, it is conjectured that this sequence has only finitely many terms.

It can be proven that

- *for a given prime number* p*, if* n *is* p*-perfect and* p *does not divide* n*, then* pn *is* $(p + 1)$*-perfect.*

□ In fact, in this case, $\sigma(n) = pn$ and $\sigma(pn) = \sigma(p)\sigma(n) = (p+1)(pn)$. In particular, if n is 3-perfect and $(3, n) = 1$, then $3n$ is 4-perfect. If n is 5-perfect and $(5, n) = 1$, then $5n$ is 6-perfect. □

On the other hand,

- *if* pn *is* $(p + 1)k$*-perfect and* $gcd(p, n) = 1$*, then* n *is* pk*-perfect.*

□ Obviously, it holds that $\sigma(pn) = ((p+1)k)(pn)$ and $\sigma(n) = \frac{((p+1)k)(pn)}{\sigma(p)} = (pk)n$. □

This implies also that

- *an integer* $2n$*, not divisible by* 4*, is a* 3*-perfect number if and only if* n *is an odd perfect number.*

On the other hand,

- *if* $3n$ *is* $4k$*-perfect and* 3 *does not divide* n*, then* n *is* $3k$*-perfect.*

It is proven that

- *any* 3*-perfect number has at least* 3 *prime divisors, any* 4*-perfect number has at least* 4 *prime divisors, any* 5*-perfect number has at least* 6 *prime divisors, any* 6*-perfect number has at least* 9 *prime divisors, and any* 7*-perfect number has at least* 14 *prime divisors.*

5.2.13. There exists another class of special numbers connected with the properties of divisibility of divisor functions. One can state that the set of multiply perfect numbers form the positive integers n under the condition $n|\sigma(n)$. It is natural to consider also the condition $\tau(n)|n$.

A *refactorable number* (or *tau number*) is an integer n that is divisible by the count of its divisors: $\tau(n)|n$.

For example, 18 has 6 divisors (1, 2, 3, 6, 9, and 6) and is divisible by 6, so 18 is refactorable.

The first few refactorable numbers are 1, 2, 8, 9, 12, 18, 24, 36, 40, 56, 60, 72, 80, 84, 88,… (sequence A033950 in the OEIS).

First defined by Cooper and Kennedy, 1990, these numbers were later rediscovered by Simon Colton, 1999. Colton got many results on refactorable numbers, proving a variety of congruence restrictions on their distribution.

In particular, Colton has showed that

- *no refactorable number is perfect.*

Also, Colton proved that

- *there are infinitely many refactorable numbers.*

However, Cooper and Kennedy proved that

- *the set of refactorable numbers have density zero.*

On the other hand, there are still unsolved problems regarding refactorable numbers. For example, it is unknown

- *if there are arbitrarily large n such that both n and $n+1$ are refactorable.*

Hyperperfect numbers

5.2.14. A *k-hyperperfect number* is a natural number n for which the equality

$$n = 1 + k(\sigma(n) - n - 1)$$

holds. Equivalently, $k\sigma(n) = (k+1)n + k - 1$. A *hyperperfect number* is a k-hyperperfect number for some positive integer k.

Hyperperfect numbers generalize perfect numbers, as

- *any perfect number is 1-hyperperfect.*

□ In fact, for a perfect number n, it holds that $1 \cdot \sigma(n) = \sigma(n) = 2n = (1+1)n + 1 - 1$. □

The first few numbers in the sequence of k-hyperperfect numbers are 6, 21, 28, 301, 325, 496, 697, 1333, 1909, 2041, 2133, 3901, 8128, 10693, 16513, ... (sequence A034897 in the OEIS), with the corresponding values of k being 1, 2, 1, 6, 3, 1, 12, 18, 18, 12, 2, 30, 1, 11, 6, ... (sequence A034898 in the OEIS). The first few k-hyperperfect numbers that are not perfect are 21, 301, 325, 697, 1333, 1909, 2041, 2133, 3901, 10693, 16513, 19521, 24601, 26977, 51301, ... (sequence A007592 in the OEIS).

The following table lists the first few k-hyperperfect numbers for small values of k, together with the sequence number in the OEIS.

k	OEIS	Some known k-hyperperfect numbers
1	*A*000396	6, 28, 496, 8128, 33550336, ...
2	*A*007593	21, 2133, 19521, 176661, 129127041, ...
3		325, ...
4		1950625, 1220640625, ...
6	*A*028499	301, 16513, 60110701, 1977225901, ...
10		159841, ...
11		10693, ...
12	*A*028500	697, 2041, 1570153, 62722153, 10604156641, 13544168521, ...
18	*A*028501	1333, 1909, 2469601, 893748277, ...
19		51301, ...
30		3901, 28600321, ...
31		214273, ...
35		306181, ...
40		115788961, ...
48		26977, 9560844577, ...
59		1433701, ...
60		24601, ...
66		296341, ...
75		2924101, ...
78		486877, ...
91		5199013, ...
100		10509080401, ...
⋮	⋮	⋮
2772	*A*028502	95295817, 124035913, ...
3918		61442077, 217033693, 12059549149, 60174845917, ...
9222		404458477, 3426618541, 8983131757, 13027827181, ...
9828		432373033, 2797540201, 3777981481, 13197765673, ...
14280		848374801, 2324355601, 4390957201, 16498569361, ...
23730		2288948341, 3102982261, 6861054901, 30897836341, ...
31752	*A*034916	4660241041, 7220722321, 12994506001, 52929885457, ...
55848		15166641361, 44783952721, 67623550801, ...
67782		18407557741, 18444431149, 34939858669, ...
92568		50611924273, 64781493169, 84213367729, ...
100932		50969246953, 53192980777, 82145123113, ...

It can be shown that

- *if* $k > 1$ *is an odd integer such that* $p = \frac{3k+1}{2}$ *and* $q = 3k+4 = 2p+3$ *are primes, then* p^2q *is* k*-hyperperfect.*

□ It is easy to obtain that $k\sigma(p^2q) = (k+1)p^2q + k - 1$. For example, for $k = 1$, we get $p = 2$, $q = 7$, and so, $p^2q = 28$, the second 1-perfect (in fact, perfect) number. For $k = 3$, we get $p = 5$, $q = 13$, and so, $p^2q = 325$, the first 3-perfect number, etc. □

In 2000, J. S. McCranie has conjectured that *all k-hyperperfect numbers for odd $k > 1$ are of this form*, but the hypothesis has not been proven so far.

Furthermore, it can be proven that

- *if $p \neq q$ are odd primes and k is an integer such that $k(p+q) = pq - 1$, then pq is k-hyperperfect.*

□ Really, it holds that

$$k\sigma(pq) = k(p+1)(q+1) = kpq + k(p+q) + k = (k+1)pq + k - 1.$$

□

For example, if $p = 3$ and $q = 5$, we get $k = 2$, and it is easy to see that 21 is 2-hyperperfect.

It is also possible to show that

- *if $k > 0$ and $p = k + 1$ is prime, then for all $\alpha > 1$ such that $q = p^\alpha - p + 1$ is prime, the number $n = p^{\alpha-1}q$ is k-hyperperfect.*

□ In fact,

$$\begin{aligned} k\sigma(p^{\alpha-1}q) &= k \cdot \frac{p^\alpha - 1}{p-1}(q+1) = k \cdot \frac{p^\alpha - 1}{k}(q+1) = (p^\alpha - 1)(q+1) \\ &= p^\alpha q - q + p^\alpha - 1 = p \cdot p^{\alpha-1}q + p - 2 \\ &= (k+1)p^{\alpha-1}q + k - 1. \end{aligned}$$

□

For example, if $k = 16$, then $p = k + 1 = 17$, and we are looking for primes q of the form $17^\alpha - 16$; in such a case, the number $n = 17^{\alpha-1}(17^\alpha - 16)$ will be 16-hyperperfect. In fact, n is 16-hyperperfect for $\alpha \in \{11, 21, 127, 149, 469, \ldots\}$. Similarly, $n = 23^{\alpha-1}(23^\alpha - 22)$ is 22-hyperperfect for $i \in \{17, 61, 445, \ldots\}$, etc.

The following table lists known values of k and corresponding values of α for which n is k-hyperperfect:

k	OEIS	Values of α
16	$A034922$	$11, 21, 127, 149, 469, \ldots$
22		$17, 61, 445, \ldots$
28		$33, 89, 101, \ldots$
36		$67, 95, 341, \ldots$
42	$A034923$	$4, 6, 42, 64, 65, \ldots$
46	$A034924$	$5, 11, 13, 53, 115, \ldots.$
52		$21, 173, \ldots$
58		$11, 117, \ldots$
72		$21, 49, \ldots$
88	$A034925$	$9, 41, 51, 109, 483, \ldots$
96		$6, 11, 34, \ldots$
100	$A034926$	$3, 7, 9, 19, 29, 99, 145, \ldots$

Almost perfect and quasi-perfect numbers

5.2.15. An *almost perfect number* (or *slightly defective number* or *least deficient number*) is a deficient number n such that $\sigma(n) = 2n - 1$.

In other words, we can say that the sum of all proper divisors of n, $s(n) = \sigma(n) - n$, is equal to $n - 1$. So, $n - s(n) = 1$, and almost perfect numbers are the deficient numbers of minimal deficiency (which is 1).

For example, the number 4 is almost perfect, as $\sigma(4) = 1 + 3 + 4 = 7 = 2 \cdot 4 - 1$.

The sequence of almost perfect numbers starts from 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, ... (sequence A000079 in the OEIS).

It is obvious that

- *any power of* 2 *with non-negative exponent is an almost perfect number.*

□ Indeed, if $n = 2^{\alpha}$, then $\sigma(n) = \sigma(2^{\alpha}) = 2^{\alpha+1} - 1 = 2 \cdot 2^{\alpha} - 1 = 2n - 1$. □

On the other hand,

- *the powers of* 2 *with non-negative exponents are the only known almost perfect numbers.*

Therefore,

- *the only known odd almost perfect number is* 1.

However, it has not been shown that all almost perfect numbers are of this form. It is proven that

- *an odd almost perfect number greater than* 1 *would have at least six prime factors.*

Moreover,

- *if* m *is an odd almost perfect number, then* $m(2m-1)$ *is a Descartes number.*

For more information, see Chapters 4 and 7.

5.2.16. A *quasi-perfect number* (or *slightly abundant number*) is an abundant number n such that $\sigma(n) = 2n + 1$.

Equivalently, $n = s(n) - 1$, i.e., the sum of its non-trivial divisors (that is, its divisors excluding 1 and n). As in this case, $s(n) - n = 1$, one can state that quasi-perfect numbers are the abundant numbers of minimal abundance (which is 1).

No quasi-perfect numbers have been found so far; in other words,

- *there are no known quasi-perfect numbers.*

If a quasi-perfect number exists, it must be of a very special form. In fact, Brown, Abbott, Aull, and Suryanarayana (1973) have proved that

- *a quasi-perfect number is an odd square number greater than* 10^{35} *and having at least seven distinct prime factors.*

5.2.17. However, there exist numbers with abundance 2, i.e., for which the sum of divisors is equal to $2n + 2$: $\sigma(n) = 2n + 2$.

The first such number is 20 since $\sigma(20) = 7 \cdot 6 = 42 == 2 \cdot 20 + 2$.

The sequence of such numbers starts from 20, 104, 464, 650, 1952, 130304, 522752, 8382464, 134193152, 549754241024, 8796086730752, 140737463189504, 144115187270549504,. . . (sequence A088831 in the OEIS).

Many of these numbers are of the form $2^{n-1}(2^n - 3)$, where $2^n - 3$ is prime (instead of $2^n - 1$ with perfect numbers). In fact, for $n = 2^{n-1}(2^n - 3)$, $2^n - 3 \in P$, it holds that

$$\begin{aligned}\sigma(n) &= \sigma(2^{n-1}(2^n - 3)) = (2^n - 1)(2^n - 2) = 2^n \cdot 2^n - 3 \cdot 2^n + 2 \\ &= 2^n(2^n - 3) + 2 = 2n + 2.\end{aligned}$$

As $2^k - 3$ is prime for $k \in \{2, 3, 4, 5, 6, 9, 10, 12, 14, 20, 22\}$, we have at least 11 solutions. There are solutions of other forms, for example, $n = 650$.

Superperfect numbers

A *superperfect number* is a positive integer n that satisfies the condition

$$\sigma^2(n) = \sigma(\sigma(n)) = 2n.$$

For example, the number 16 is a superperfect number, as $\sigma(16) = 1 + 2 + 4 + 8 + 16 = 31$, and $\sigma(31) = 1 + 31 = 32$; thus, $\sigma(\sigma(16)) = 32 = 2 \cdot 16$.

The first few superperfect numbers are 2, 4, 16, 64, 4096, 65536, 262144, 1073741824,. . . (sequence A019279 in the OEIS).

The only known superperfect numbers are those powers of 2 that lead to the Mersenne primes. In fact,

- *if* $M_p = 2^p - 1$ *is a Mersenne prime, then* $n = 2^{p-1}$ *is superperfect.*

□ It is obvious because in this case, it holds that

$$\sigma(n) = \sigma(2^{p-1}) = 2^p - 1, \quad \text{and} \quad \sigma(2^p - 1) = 2^p = 2n. \qquad \square$$

For example,

$$\sigma(\sigma(2)) = \sigma(3) = 4 = 2 \cdot 2;\ \sigma(\sigma(4)) = \sigma(7) = 8 = 2 \cdot 4,$$
$$\sigma(\sigma(16)) = \sigma(31) = 32 = 2 \cdot 16;$$
$$\sigma(\sigma(64)) = \sigma(127) = 128 = 2 \cdot 64;$$
$$\sigma(\sigma(4096)) = \sigma(8191) = 8192 = 2 \cdot 4096.$$

Conversely, any even superperfect number should have the following form:

- *If n is an even superperfect number, then $n = 2^k$ such that $2^{k+1} - 1$ is a Mersenne prime.*

It is not known whether there are any odd superperfect numbers. At present, it is checked that there are no odd superperfect numbers below $7 \cdot 10^{24}$. If odd superperfect numbers exist, they should be large and of special form. It is proven that

- *any odd superperfect number n should be a square number such that either n or $\sigma(n)$ is divisible by at least three distinct primes.*

5.2.18. An *almost superperfect number* is a positive integer n that satisfies the condition

$$\sigma^2(n) = \sigma(\sigma(n)) = 2n - 1.$$

- *No almost superperfect numbers have been found yet.*

A *quasi-superperfect number* is a positive integer n that satisfies the condition

$$\sigma^2(n) = \sigma(\sigma(n)) = 2n + 1.$$

- *The known quasi-superperfect numbers are just the Mersenne primes.*

□ It is easy to show that any Mersenne prime is quasi-superperfect. In fact, if $M_p = 2^p - 1 \in P$, then

$$\sigma(M_p) = \sigma(2^p - 1) = 2^p, \quad \text{and}$$
$$\sigma(2^p) = 2^{p+1} - 1 = 2 \cdot (2^p - 1) + 1 = 2 \cdot M_p. \qquad \square$$

5.2.19. Perfect and superperfect numbers are examples of a wider class of the so-called *m-superperfect numbers*, which satisfy the condition

$$\sigma^m(n) = 2n, \quad \text{where} \ \ \sigma^1(n) = \sigma(n),$$
$$\sigma^2(n) = \sigma(\sigma(n)), \ldots, \sigma^m(n) = \sigma(\sigma^{m-1}(n)).$$

In this notation, perfect numbers correspond to $m = 1$ and superperfect numbers to $m = 2$.

Now, the reader can define *quasi m-superperfect* and *almost m-superperfect numbers* as follows: *quasi m-superperfect numbers* satisfy the condition $\sigma^m(n) = 2n + 1$, while *almost m-superperfect numbers* satisfy the condition $\sigma^m(n) = 2n - 1$.

5.2.20. The m-superperfect numbers are in turn examples of *(m, k)-perfect numbers*, which satisfy the condition

$$\sigma^m(n) = kn.$$

With this notation, perfect numbers are (1,2)-perfect, multiply perfect numbers are $(1, k)$-perfect, superperfect numbers are $(2, 2)$-perfect, and m-superperfect numbers are $(m, 2)$-perfect.

Examples of classes of (m, k)-perfect numbers are given in the following table.

m	k	(m, k)-perfect numbers	OEIS
2	2	2, 4, 16, 64, 4096, 65536, 262144	A019279
2	3	8, 21, 512	A019281
2	4	15, 1023, 29127	A019282
2	6	42, 84, 160, 336, 1344, 86016,...	A019283
3	any	12, 14, 24, 52, 98, 156, 294,...	A019292
4	any	2, 3, 4, 6, 8, 10, 12, 15, 18, 21,...	A019293

For example, the number 12 is $(3, 10)$-perfect number, as

$$\sigma(12) = 28, \ \sigma(28) = 56, \ \sigma(56) = 120 = 10 \cdot 12.$$

The number 2 is $(4, 4)$-perfect number, as

$$\sigma(2) = 3, \ \sigma(3) = 4, \ \sigma(4) = 7, \ \sigma(7) = 8 = 4 \cdot 2.$$

The number 3 is $(4,5)$-perfect number, as

$$\sigma(3) = 4,\ \sigma(4) = 7,\ \sigma(7) = 8,\ \sigma(8) = 15 = 5 \cdot 3.$$

Quasi (m,k)-perfect and almost (m,k)-perfect numbers can be defined now similarly as follows: A *quasi* (m,k)*-perfect number* satisfies the condition $\sigma^m(n) = kn + 1$, while an *almost* (m,k)*-perfect number* satisfies the condition $\sigma^m(n) = kn - 1$. The reader can try to find some examples of such special numbers.

$\mathcal{S}$-perfect numbers

5.2.21. In number theory, $\mathcal{S}$*-perfect numbers* (or *Granville numbers*) are an extension of the perfect numbers.

In 1996, A. Granville proposed the following construction of a set $\mathcal{S}$:

Let $1 \in \mathcal{S}$, and for any integer n larger than 1, let $n \in \mathcal{S}$ if

$$\sum_{d|n, d<n, d\in\mathcal{S}} d \le n.$$

An $\mathcal{S}$*-perfect number* (or *Granville number*) is an element of $\mathcal{S}$ for which equality holds. That is, n is a $\mathcal{S}$-perfect number if it is equal to the sum of its proper divisors that are also in $\mathcal{S}$:

$$\sum_{d|n, d<n, d\in\mathcal{S}} d = n.$$

It is easy to see that 6 is the first $\mathcal{S}$-perfect number. In fact, as $1 \in \mathcal{S}$, then the numbers 2, 3, 4, and 5 belong to $\mathcal{S}$ and are under the condition $\sum_{d|n,d<n,d\in\mathcal{S}} d < n$:

$$1 < 2,\ 1 < 3,\ 1 + 2 = 3 < 4,\ 1 < 5.$$

However, for 6, it holds that $\sum_{d|n,d<n,d\in\mathcal{S}} d = n$:

$$\sum_{d|6, d<6, d\in\mathcal{S}} d = 1 + 2 + 3 = 6.$$

The first few $\mathcal{S}$-perfect numbers are 6, 24, 28, 96, 126, 224, 384, 496, 1536, 1792, 6144, 8128, 14336, 15872, 24576,... (sequence A118372 in the OEIS).

It is obvious that *any deficient and any perfect number belong to* $\mathcal{S}$:

- *For a given positive integer* n*, if* $s(n) \leq n$*, then* $n \in \mathcal{S}$*.*

□ In fact, the restriction of the divisors sum to members of $\mathcal{S}$ either decreases the divisors sum or leaves it unchanged. So,

$$\sum_{d|n, d<n, d\in\mathcal{S}} d \leq \sum_{d|n, d<n} d = s(n) \leq n. \qquad \square$$

In particular,

- *for a given distinct primes* p, q *and any* $\alpha \in \mathbb{N}$*, it holds that* p^α*,* $pq \in \mathcal{S}$*.*

It is easy to see that for any deficient number, the inequality is strict in the condition above. However,

- *every perfect number is also* $\mathcal{S}$*-perfect.*

□ Due to the multiplicativity of $\sigma(n)$, it holds that $\frac{\sigma(d)}{d} \leq \frac{\sigma(n)}{n}$ for any divisor d of n, and the inequality is strict if $d < n$. So, for any proper divisor d of a perfect number n, it holds that $\sigma(d) - d < d$, i.e., d is deficient and hence belongs to $\mathcal{S}$. So, for any perfect number n, we get

$$\sum_{d|n, d<n, d\in\mathcal{S}} d = \sum_{d|n, d<n} d = s(n) = n,$$

i.e., n is $\mathcal{S}$-perfect. □

But there are numbers, such as 24, which are $\mathcal{S}$-perfect but not perfect. In fact (see [KoIv96]),

- *the number* $n = 2^\alpha p$ *with odd prime* p *is* $\mathcal{S}$*-perfect if and only if* $p = 2^r - 1$*, i.e., is an Mersenne prime and* $\alpha = kr - 1$*,* $k \in \mathbb{N}$*.*

For example, $24 = 2^3 \cdot 3 = 2^\alpha p$, where $p = 3 = M_2 = 2^2 - 1$ and $\alpha = 3 = 2 \cdot 2 - 1$; $96 = 2^5 \cdot 3 = 2^\alpha p$, where $p = 3 = M_2 = 2^2 - 1$ and $\alpha = 5 = 3 \cdot 2 - 1$, etc.

Moreover, it is proven in [KoIv96] that

- *the only $\mathcal{S}$-perfect number of the form* $2 \cdot 3^2 \cdot p$, *where* $p \in p, gcd(6,p) = 1$, *is* $126 = 2 \cdot 3^2 \cdot 7$.

In fact, 126 is the only known $\mathcal{S}$-perfect number with three distinct prime factors.

Numbers that fulfill the strict form of the inequality in the above definition are known as *$\mathcal{S}$-deficient numbers*. That is, *$\mathcal{S}$-deficient numbers* are the natural numbers for which the sum of their divisors in $\mathcal{S}$ is strictly less than themselves:

$$\sum_{d|n,\ d<n,\ d\in\mathcal{S}} d < n.$$

The first few $\mathcal{S}$-deficient numbers are: 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 13, 14, 15, 16, ...

Numbers that violate the inequality in the above definition are known as *$\mathcal{S}$-abundant numbers.* That is, the *$\mathcal{S}$-abundant numbers* are positive integers for which the sum of their divisors in $\mathcal{S}$ is strictly greater than themselves:

$$\sum_{d|n,\ d<n,\ d\in\mathcal{S}} d > n.$$

These numbers form the complement of $\mathcal{S}$. The first few $\mathcal{S}$-abundant numbers are: 12, 18, 20, 30, 42, 48, 56, 66, 70, 72, 78, 80, 84, 88, 90, 102, 104, ... (sequence A181487 in the OEIS).

The first positive integer that is not in $\mathcal{S}$ is the smallest abundant number 12. The next two abundant numbers, 18 and 20, are also not in $\mathcal{S}$. However, the fourth abundant number, 24, is in $\mathcal{S}$ because the sum of its proper divisors in $\mathcal{S}$ is: $1+2+3+4+6+8 = 24$. In other words, 24 is abundant but not $\mathcal{S}$-abundant because 12 is not in $\mathcal{S}$. In fact, 24 is $\mathcal{S}$-perfect, and it is the smallest number that is $\mathcal{S}$-perfect but not perfect.

The smallest odd abundant number that is in $\mathcal{S}$ is 2835, and the smallest pair of consecutive numbers that are not in $\mathcal{S}$ are 5984 and 5985 [KoIv96].

Unitary perfect numbers

5.2.22. A positive integer divisor d of a positive integer n is called an *unitary divisor* if d and $\frac{n}{d}$ share no common factors. In other words, if the prime decomposition of n has the form $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, then all unitary divisors of n are

$$1, p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}, p_1^{\alpha_1} p_2^{\alpha_2}, \ldots, p_1^{\alpha_1} p_k^{\alpha_k}, \ldots, p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}.$$

The concept of unitary divisor was originally due to R. Vaidyanathaswamy (1931), who called such a divisor *block factor*. The present terminology is due to E. Cohen (1960).

The sum of the unitary divisors of n is denoted by $\sigma^*(n)$. It is a multiplicative function with $\sigma^*(p^\alpha) = p^\alpha + 1$ (see sequence A034448 in the OEIS).

A *unitary perfect number* is a positive integer which is the sum of its positive proper unitary divisors, not including the number itself, i.e., a number n for which it holds that

$$\sigma^*(n) = 2n.$$

For example, the number $60 = 2^2 \cdot 3 \cdot 5$ is a unitary perfect number because 1, 3, $4 = 2^2$, 5, $12 = 2^2 \cdot 3$, $15 = 3 \cdot 5$, and $20 = 2^2 \cdot 5$ are its proper unitary divisors, and

$$1 + 3 + 4 + 5 + 12 + 15 + 20 = 60.$$

The first five, and only known, unitary perfect numbers are

$$6, 60, 90, 87360, \text{ and } 146361946186458562560000$$

(sequence A002827 in the OEIS).

In fact, $6 = 2 \cdot 3$, $60 = 2^2 \cdot 3 \cdot 5$, $90 = 2 \cdot 3^2 \cdot 5$ $87360 = 2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 13$, and $146361946186458562560000 = 2^{18} \cdot 3 \cdot 5^4 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 37 \cdot 79 \cdot 109 \cdot 157 \cdot 313$, while the respective sums of proper unitary divisors are as follows (4095 divisors in the last sum):

$$\begin{aligned}
6 &= 1+2+3;\ 60 = 1+3+4+5+12+15+20;\\
90 &= 1+2+5+9+10+18+45;\\
87360 &= 1+3+5+7+13+15+21+35+39+64+65\\
&\quad +91+105+192+195+273+320+448+455+832\\
&\quad +960+1344+1365+2240+2496+4160+5824\\
&\quad +6720+12480+17472+29120;\\
&\quad 146361946186458562560000 = 1+3+5+6+7\\
&\quad +11+13+19+\cdots+13305631471496232960000\\
&\quad +20908849455208366080000+48787315395486187520000.
\end{aligned}$$

It is easy to see that

- *there are no odd unitary perfect numbers.*

□ This follows since $2^{\nu(n)}$ divides the sum of the unitary divisors of an odd number n, where $\nu(n)$ is the number of distinct prime divisors of n. One gets this because the sum of all the unitary divisors is a multiplicative function and one has the sum of the unitary divisors of a power p^α of a prime p equal to $p^\alpha + 1$ which is even for any odd prime p. Therefore, an odd unitary perfect number must have only one distinct prime factor, and it is not hard to show that a power of prime cannot be a unitary perfect number since there are not enough divisors. □

It is not known *whether or not there are infinitely many unitary perfect numbers* or indeed *whether there are any further examples beyond the five already known.* It is proven that

- *a unitary perfect number greater than* 146361946186458562560000 *would have at least nine odd prime factors.*

5.2.23. Using the notion of unitary perfect numbers, one can see that several extensions can be made for this class of numbers.

So, a positive integer n is called a *unitary k-perfect number* if

$$\sigma^*(n) = kn,\ \ k \in \mathbb{N}.$$

An *unitary multiply perfect number* is thus simply a unitary k-perfect number for some positive integer k.

Equivalently, unitary multiply perfect numbers are those n for which n divides $\sigma^*(n)$.

So, in this terminology, the unitary perfect numbers are just unitary 2-perfect numbers.

In the case $k > 2$, no example of a unitary k-perfect number is known. It is proven that if such a number exists, it must be an even number greater than 10^{102} and must have more than 44 odd prime factors.

5.2.24. Similarly, one can construct and study the so-called *bi-unitary multiply perfect numbers*.

A positive integer divisor d of a positive integer n is called a *bi-unitary divisor* of n if the greatest common unitary divisor of d and $\frac{n}{d}$ is equal to 1.

This concept is due to D. Surynarayana (1969).

The sum of the bi-unitary divisors of n is denoted by $\sigma^{**}(n)$ (see sequence A188999 in the OEIS). It is a multiplicative function with $\sigma^{**}(p^\alpha) = \sigma(p^\alpha) = \frac{p^{\alpha+1}-1}{p-1}$ for odd α, and $\sigma^{**}(p^\alpha) = \sigma(p^\alpha) - p^{\alpha/2} = \frac{p^\alpha-1}{p-1}(p^{\alpha+1}+1)$ for even α.

A positive integer n is called a *bi-unitary k-perfect number* if

$$\sigma^{**}(n) = kn,\ \ k \in \mathbb{N}.$$

Then, a *bi-unitary multiply perfect number* is simply a bi-unitary k-perfect number for some positive integer k. In other words, bi-unitary multiply perfect numbers are those n for which n divides $\sigma^{**}(n)$.

The first bi-unitary multiply perfect numbers are 1, 6, 60, 90, 120, 672, 2160, 10080, 22848, 30240, 342720, 523776, 1028160, 1528800, 6168960,... (sequence A178000 in OEIS).

In this terminology, a bi-unitary 2-perfect number is naturally called a *bi-unitary perfect number*; it is a positive integer which is equal to the sum of its bi-unitary proper divisors. The only such numbers are 6, 60, and 90 (Wall, 1972).

P. Hagis (1987) proved that

- *there are no odd bi-unitary multiply perfect numbers.*

Haukkanen and Sitaramaiah (2020) found certain even bi-unitary 3-perfect numbers, including all such numbers up to $8 \cdot 10^{10}$, as well as all bi-unitary 4-perfect numbers in this range.

Perfect totient numbers

5.2.25. A *perfect totient number* is a positive integer that is equal to the sum of its iterated totients. That is, for a given n, we apply the Euler's totient function to the number n, apply it again to the resulting totient, and so on, until the number 1 is reached and add together the resulting sequence of numbers; if the obtained sum is equal to n, then n is a perfect totient number.

For example, there are two positive integers less than 3 and relatively prime to it, so the totient of 3 is 2; there is one number less than 2 and relatively prime to it, so the totient of 2 is 1; as $3 = 2 + 1$, we can state that the number 3 is a perfect totient number. Similarly, there are six positive integers less than 9 and relatively prime to it, so the totient of 9 is 6; there are two numbers less than 6 and relatively prime to it, so the totient of 6 is 2; and there is one number less than 2 and relatively prime to it, so the totient of 2 is 1; as $9 = 6 + 2 + 1$, we can state that the number 9 is a perfect totient number.

The first few perfect totient numbers are 3, 9, 15, 27, 39, 81, 111, 183, 243, 255, 327, 363, 471, 729, 2187,... (sequence A082897 in the OEIS).

Formally, let

$$\phi^i(n) = \begin{cases} \phi(n), & \text{if } i = 1; \\ \phi(\phi^{i-1}(n)), & \text{if } i \geq 2. \end{cases}$$

Then, one has that n is a perfect totient number if

$$n = \sum_{i \geq 1} \phi^i(n).$$

It can be observed that many perfect totient are multiples of 3 (in fact, 4375 is the smallest perfect totient number that is not divisible by 3). Moreover, it is easy to show that

- *all positive powers of* 3*, i.e., all the numbers of the form* $3^\alpha, \alpha \in \mathbb{N}$*, are perfect totient numbers.*

□ Really, it can be proven by induction using the fact that

$$\phi(3^\alpha) = \phi(2 \cdot 3^\alpha) = 2 \cdot 3^{\alpha-1}.$$

So,

$$\phi(3^\alpha) = 2 \cdot 3^{\alpha-1},\ \phi(2 \cdot 3^{\alpha-1}) = \phi(3^{\alpha-1}) = 2 \cdot 3^{\alpha-2}, \ldots, \phi(2 \cdot 3) = 2, \quad \text{and}\ \ \phi(2) = 1.$$

Now, we get that

$$1 + 2 + 2 \cdot 3 + \cdots + 2 \cdot 3^{\alpha-1} = 1 + 2 \cdot \frac{3^\alpha - 1}{2} = 3^\alpha.$$

The property is proved. □

Venkataraman (1975) found another family of perfect totient numbers:

- *If* $p = 4 \cdot 3^\alpha + 1$ *is prime, then* $3p$ *is a perfect totient number.*

The values of α leading to perfect totient numbers in this way are 0, 1, 2, 3, 6, 14, 15, 39, 201, 249, 1005, 1254, 1635,... (sequence A005537 in the OEIS).

It is not known

- *whether there exists any perfect totient number of the form* $3^\alpha p$*, where* p *is a prime and* $\alpha > 3$*.*

For references and some additional information, see, for example, [BeEr74], [Melf15], [Krav76], [Erdo73], [ChZh11], [ErNi75], [CoKe90], [Colt99], [Zeli02], [BAAS73], [Sury69], [Weis22], [CoRi96], [Guy94], [Koni09], [KoIv96], [Wall72], [MSC96], [Deza21], [Yan96], [Weis22], [Wiki22], and [Sloa22].

Exercises

1. Check that numbers 2, 5, and 52 are untouchable.
2. Check that 24 is an Erdős–Nicolas number.
3. Check that 1 is 1-perfect, 6 is 2-perfect, 120 is 3-perfect, and 30240 is 4-perfect.
4. Check that 8 is a refactorable number; find the first five refactorable numbers.
5. Check that 9 is a perfect totient number. Prove that 3, 9, 15, 27, 39, and 81 are the only perfect totient numbers less than 100. Prove that if $p = 4 \cdot 3^{\alpha} + 1$ is prime, then $3p$ is a perfect totient number.
6. Prove that the only one- and two-digit $\mathcal{S}$-perfect numbers are 6, 24, 28, and 96.
7. Check that all known 3-perfect numbers have at least 3 prime factors, all known 4-perfect numbers have at least 4 prime factors, all known 5-perfect numbers have at least 6 prime factors, all known 6-perfect numbers have at least 9 prime factors, and all known 7-perfect numbers have at least 14 prime factors.
8. Prove that if n is a 3-perfect number, $3|n$, but $5 \not| n$ and $9 \not| n$, then $45n$ is 4-perfect.
9. Prove that if n is a 5-perfect number and $3|n$, then $3n$ is 4-perfect.
10. Prove that if $3n$ is a k-perfect number and $3 \not| n$, then n is $3k$-perfect.
11. Check that $14182439040 = 2^7 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11^2 \cdot 17 \cdot 19$ is a 5-perfect number (in fact, it is the first 5-perfect number).

5.3. Relatives of Amicable Numbers

Amicable tuples

5.3.1. Recall that amicable numbers (m, n) can be defined by the conditions $\sigma(m) - m = n$ and $\sigma(n) - n = m$, which can be written together as

$$\sigma(m) = \sigma(n) = m + n.$$

As a simple generalization, we can consider larger tuples, say $(n_1, n_2, \dots, n_k)$, where we require

$$\sigma(n_1) = \sigma(n_2) = \cdots = \sigma(n_k) = n_1 + n_2 + \cdots + n_k.$$

All such finite multisets $(n_1, n_2, \dots, n_k)$ are called *amicable multisets.*

If all members of an amicable k-multiset coincide, we obtain the definition of k-perfect numbers; for example, for the triple $(120, 120, 120)$, the above condition holds, as 120 is 3-perfect: $\sigma(120) = 360 = 3 \cdot 120 = 120 + 120 + 120$ (compare with the perfect number 6, which form a degenerate amicable pair $(6, 6)$). The triple $(1740, 1740, 1560)$ with the property

$$\sigma(1740) = \sigma(1560) = 5040 = 1740 + 1740 + 1560$$

has two equal members, while the members of the triple (1980, 2016, 2556) with the property $\sigma(1980) = \sigma(2016) = \sigma(2556) = 6552 = 1980 + 2016 + 2556$ are pairwise distinct.

So, in order to obtain a non-trivial construction, similar to the construction of amicable pairs, we define an *amicable k-tuple*, $k \in \mathbb{N}, k \geq 2$, as a k-tuple $(n_1, n_2, \dots, n_k)$ of positive integers $n_1, n_2, \dots, n_k$ such that

$$\sigma(n_1) = \sigma(n_2) = \cdots = \sigma(n_k) = n_1 + n_2 + \cdots + n_k,$$
$$\text{and} \quad n_1 < n_2 < \cdots < n_k.$$

For $k = 2$, we get the definition of amicable numbers. So, one can state that

- *any amicable pair is an amicable* 2*-tuple.*

For $k = 3$, we get the set of amicable triples.

The smallest amicable triple is (1980, 2016, 2556). As was shown before, it holds that $\sigma(1980) = \sigma(2016) = \sigma(2556) = 6552 = 1980 + 2016 + 2556$. The next one is $(9180, 9504, 11556)$.

The first 10 amicable triples (x, y, z), $x < y < z$, are represented in the following table.

A125490	x	1980	9180	21168	23940	37380	38940	38940	39480	46368	47124
A125491	y	2016	9504	22200	31284	41412	40068	40608	43890	54990	52290
A125492	z	2556	11556	27312	32136	42168	41952	41412	54870	55890	57834
A137231	$\sigma(x)$	6552	30240	70680	87360	120960	120960	120960	138240	157248	157248

The smallest amicable quadruple is (3270960, 3361680, 3461040, 3834000). It is easy to check that

$$\sigma(3270960) = \sigma(3361680) = \sigma(3461040) = \sigma(3834000)$$
$$= 13927680 = 3270960, +3361680 + 3461040 + 3834000.$$

The next one is $(3767400, 4090320, 4150440, 4240800)$.

The first 10 amicable quadruples (x, y, z, u), $x < y < z < u$, are represented in the following table.

A036471	A036472	A036473	A036474	A116148
x	y	z	u	$\sigma(x)$
3270960	3361680	3461040	3834000	13927680
3767400	4090320	4150440	4240800	16248960
4651920	4839120	4918320	5089392	19498752
4969440	5116320	5475960	5666760	21228480
5682600	5831280	5920200	6939360	24373440
5405400	6029100	6421800	7142100	24998400
6514200	6640200	6768720	7932240	27855360
6126120	6541920	7559640	8076960	28304640
6126120	6922080	7280280	7976160	28304640
6320160	6902280	7685496	8122464	29030400

In order to obtain some new amicable triples, one can use the following rule:

- *If (a, b) and (x, y) are amicable pairs and $gcd(a, x) = gcd(a, y) = gcd(b, x) = gcd(b, y) = 1$, then (ax, ay, bx, by) is an amicable quadruple.*

☐ In fact, it holds that

$$\sigma(ax) = \sigma(a)\sigma(x) = (a + b)(x + y) = ax + ay + bx + by.$$

Moreover, $\sigma(ax) = \sigma(a)\sigma(x) = \sigma(b)\sigma(x) = \sigma(bx)$; the conditions $\sigma(ax) = \sigma(ay) = \sigma(by)$ can be obtained similarly. $\square$

One can find some large amicable quadruples using the following rule:

$$\begin{aligned}(a, b, c, d) = C_p(&173 \cdot 1933058921 \cdot 149 \cdot 103540742849, 173\\ &\cdot 1933058921 \cdot 15531111427499, 336352252427\\ &\cdot 149 \cdot 103540742849, 336352252427 \cdot 15531111427499),\end{aligned}$$

where M_p *is a Mersenne prime with* $p > 3$ *and*

$$\begin{aligned}C_p = 2^{p-1}M_p &\cdot 5^9 \cdot 7^2 \cdot 11^4 \cdot 17^2 \cdot 19^1 \cdot 29^2 \cdot 67 \cdot 71^2 \cdot 109 \cdot 131 \cdot 139\\ &\cdot 179 \cdot 307 \cdot 431 \cdot 521 \cdot 653 \cdot 1019 \cdot 1279 \cdot 2557 \cdot 3221\\ &\cdot 5113 \cdot 5171 \cdot 6949.\end{aligned}$$

The sequence A259307 in the OEIS collects the numbers that belong to at least one amicable multiset. They start from 1, 6, 28, 120, 220, 284, 496, 672, 1184, 1210, 1560, 1740, 1980, 2016, ...

Friendly numbers

5.3.2. The *abundancy* (or *abundancy index*) of a positive integer n is defined as the rational number $I(n) = \frac{\sigma(n)}{n}$. It is not the same as *abundance*, which is defined as $\sigma(n) - 2n$.

A positive integer n is called a *friendly number* if there exists a positive integer $m \neq n$ such that $\frac{\sigma(m)}{m} = \frac{\sigma(n)}{n}$. Otherwise, n is called *solitary number*.

In other words, *friendly numbers* are defined as two or more positive integers with a common abundancy. Two numbers with the same abundancy form a *friendly pair*; k numbers with the same abundancy form a *friendly k-tuple*.

Note that there exist other interpretations of this term. For example, Hoffman (1998) uses the term "friendly numbers" to describe amicable pairs.

For example, friendly pairs can be represented by

$$(6, 28), (30, 140), (80, 200), (40, 224), (12, 234), (84, 270), (66, 308), \ldots;$$

friendly triples can be represented by

$$(2160, 5400, 13104), (9360, 21600, 23400), (4320, 4680, 26208), \ldots;$$

friendly quadruples by

$$(6, 28, 496, 8128), (3612, 11610, 63984, 70434),$$
$$(3948, 12690, 69936, 76986), \ldots;$$

and friendly 5-tuples by

$$(84, 270, 1488, 1638, 24384), (30, 140, 2480, 6200, 40640),$$
$$(420, 7440, 8190, 18600, 121920), \ldots.$$

Obviously, "being mutually friendly" is an equivalence relation and thus induces a partition of the positive integers into *clubs* (equivalence classes) of mutually friendly numbers. So, for a solitary number which, by definition, is not part of any friendly pair, its club consists only of itself.

As the numbers 1 through 5 are all solitary (since $gcd(\sigma(n), n) = 1$ for $n = 1, 2, 3, 4, 5$, see the following corresponding property), then the smallest friendly number is 6, forming, for example, the friendly pair $(6, 28)$ with abundancy $I(6) = \frac{\sigma(6)}{6} = \frac{1+2+3+6}{6} = 2$, the same as $I(28) = \frac{\sigma(28)}{28} = \frac{1+2+4+7+14+28}{2} = 2$. Numbers with abundancy 2 are also known as perfect numbers. So, all perfect numbers are friendly with each other, forming a friendly group. The shared value 2 is an integer in this case but not in many other cases. In fact, numbers with abundancy k, $k \in \mathbb{N}$, are known as k-perfect numbers.

On the other hand, in spite of the similarity in name, there is no specific relationship between the friendly numbers and the amicable numbers, although the definitions of both the classes of numbers involve the divisor function.

In general, $I(n)$ is not an integer. So, the friendly pair (4320, 4680) has the abundancy $3,5$:

$$I(4320) = \frac{\sigma(4320)}{4320} = \frac{15120}{4320} = \frac{7}{2}, \quad \text{and}$$
$$I(4680) = \frac{\sigma(4680)}{4680} = \frac{16380}{4680} = \frac{7}{2}.$$

As another example, the numbers 30 and 140 form a friendly pair $(30, 140)$ because 30 and 140 have the same abundancy $2,4$:

$$\frac{\sigma(30)}{30} = \frac{1+2+3+5+6+10+15+30}{30} = \frac{72}{30} = \frac{12}{5};$$
$$\frac{\sigma(140)}{140} = \frac{1+2+4+5+7+10+14+20+28+35+70+140}{140}$$
$$= \frac{336}{140} = \frac{12}{5}.$$

The numbers 2480, 6200, and 40640 are also members of this club.

For an example of odd numbers being friendly, consider the pair (135, 819) with abundancy $\frac{16}{9}$ (as it is less then 2, both numbers are deficient).

There are also cases of even being friendly to odd, such as the pair (42, 544635) with abundancy $\frac{16}{7}$.

The odd friend may be less than the even one, as in the pair $(84729645, 155315394)$ with abundancy $\frac{896}{351}$.

A square number can be friendly. For instance (Hickerson), both 693479556 (the square of 26334) and 8640 have abundancy $\frac{127}{36}$.

Small numbers with a relatively large smallest friend do exist: For instance, 24 is friendly, with its smallest friend 91963648. The friendly pair $(24, 91963648)$ has abundancy $2,5$.

The sequence of known friendly numbers starts with 6, 12, 24, 28, 30, 40, 42, 56, 60, 66, 78, 80, 84, 96, 102,… (sequence A074902 in the OEIS).

5.3.3. A *solitary number* is a number that belongs to a singleton club because no other number is friendly with it.

All prime numbers are known to be solitary as are powers of prime numbers. More generally,

- *if the numbers n and $\sigma(n)$ are coprime so that $\frac{\sigma(n)}{n}$ is an irreducible fraction, then the number n is solitary.*

□ In fact, if $gcd(\sigma(n), n) = 1$ and there are $m \neq n$ such that $\frac{\sigma(n)}{n} = \frac{\sigma(m)}{m}$, then $m\sigma(n) = n\sigma(m)$, $m = kn$, and $\sigma(m) = k\sigma(n)$, $k \in \mathbb{N}$; for $k > 1$, it is impossible, as $\sigma(kn) > k\sigma(n)$. For a prime number p, we have $\sigma(p) = p + 1$, which is coprime with p. Similarly, $\sigma(p^\alpha) = 1 + p + \cdots + p^\alpha$ also is coprime with p. □

The first numbers under the condition $gcd(\sigma(n), n) = 1$ are 1, 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 21, 23,... (sequence A014567 in the OEIS).

However, there exist solitary numbers n for which $(\sigma(n), n) > 1$. The list of known such numbers is thus: 18, 45, 48, 52, 136, 148, 160, 162, 176, 192, 196, 208, 232, 244, 261, 272, 292, 296, 297, 304, 320, 352, 369 (sequence A095739 in the OEIS).

On the other hand, the classification of numbers 10, 14, 15, 20, 22, 26, 33, 34, 38, 44, 46, 51, 54, 58, 62, 68, 69, 70, 72, 74, 76, 82, 86, 87, 88, 90, 91, 92, 94, 95, 99, 104, 105,... is still unknown.

No general method exists for determining whether a number is friendly or solitary. The smallest number whose classification is unknown is 10; it is conjectured to be solitary. If it is not, its smallest friend is at least 10^{30}.

5.3.4. It is easy to show that every pair (m, n) of friendly numbers gives rise to a positive proportion of all positive integers being friendly (but in different clubs) by considering pairs (km, kn) for multiple k with $gcd(k, mn) = 1$.

For example, the *primitive friendly pair* $(6, 28)$ gives rise to friendly pairs $(6k, 28k)$ for all k coprime with 42, i.e., congruent to 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, or 41 modulo 42; The common abundancy of the pair $(6k, 28k)$ is $\frac{2\sigma(k)}{k}$.

So, we have proven that

- *there are infinitely many friendly numbers.*

This leads to the proposition that *the density of the friendly numbers (if it exists) is positive.*

Anderson and Hickerson proposed that the density should in fact be 1 (or, equivalently, that the density of the solitary numbers should be 0). This conjecture has not been resolved.

However, it is an open problem whether there are infinitely large clubs of mutually friendly numbers. Perfect numbers form a club, and it is conjectured that there are infinitely many perfect numbers (at least as many as there are Mersenne primes), but no proof is known. As of 2021, 51 perfect numbers are known, the largest of which has more than 49 million digits.

There are clubs with more known members: in particular, those formed by k-perfect numbers, which are numbers whose abundancy is an integer k. As of early 2013, the club of friendly numbers with abundancy equal to 9 has 2094 known members. Although some of such classes are known to be quite large, clubs of multiply perfect numbers (excluding the perfect numbers themselves) are conjectured to be finite.

Multiple amicable numbers

5.3.5. Two positive integers (m, n), $m < n$, are called an (α, β)-*multiple amicable pair* (or (α, β)-*multiple amicable pair*), $\alpha, \beta \in \mathbb{N}$, if

$$\sigma(m) - m = \alpha n \quad \text{and} \quad \sigma(n) - n = \beta m.$$

Equivalently, we get a multiple amicable pair (m, n) if

$$\sigma(m) = \alpha n + m, \quad \text{and } \sigma(n) = \beta m + n, \alpha, \beta \in \mathbb{N}.$$

In general, the condition $\alpha\beta > 1$ is used since if $\alpha = \beta = 1$, we get an ordinary amicable pair.

For example, the pair (52920, 152280) is $(1, 7)$-multiple amicable since

$$\sigma(52920) = 152280 + 52920 \quad \text{and } \sigma(152280) = 6 \cdot 52920 + 152280,$$

while the pair (76455288, 183102192) is $(1, 6)$-multiple amicable since

$$\sigma(76455288) = 76455288 + 183102192 \quad \text{and}$$
$$\sigma(183102192) = 6 \cdot 76455288 + 183102192.$$

In 1995, Cohen, Gretton, and Haggis have used an exhaustive numerical method to find the following six (α, β)-amicable pairs (m, n) with $m \leq 10^8$:

- *There are three* $(1, 7)$*-amicable pairs* (m, n)*, the pairs are*

$$(m = 52920 = 2^3 \cdot 3^3 \cdot 5 \cdot 7^2,$$
$$n = 152280 = 2^3 \cdot 3^4 \cdot 5 \cdot 47);$$
$$(m = 16225560 = 2^3 \cdot 3^2 \cdot 5 \cdot 13 \cdot 3467,$$
$$n = 40580280 = 2^3 \cdot 3^2 \cdot 5 \cdot 13^2 \cdot 23 \cdot 29);$$
$$(m = 90863136 = 2^5 \cdot 3^2 \cdot 7 \cdot 13 \cdot 3467,$$
$$n = 227249568 = 2^5 \cdot 3^2 \cdot 7 \cdot 13^2 \cdot 23 \cdot 29).$$

- *There are two* $(2, 5)$*-amicable pairs* (m, n)*, the pairs are*

$$(m = 3598560 = 2^5 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 17,$$
$$n = 5957280 = 2^5 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 197);$$
$$(m = 3598560 = 2^3 3^2 5^1 7^2 13^1 17,$$
$$n = 5957280 = 2^3 3^2 5^1 7^2 13^1 197).$$

- *There is one* $(1, 6)$*-amicable pair* (m, n)*, the pair is*

$$(m = 76455288 = 2^3 \cdot 3^2 \cdot 7^2 \cdot 13 \cdot 1667,$$
$$n = 183102192 = 2^4 \cdot 3^2 \cdot 7 \cdot 13 \cdot 89 \cdot 157).$$

5.3.6. It is easy to see that

- *for an* (α, β)*-multiple amicable pair, it holds that*

$$(\alpha + 1)m < \sigma(m) < (\alpha + 1)n, \quad \textit{and} \quad (\beta + 1)n < \sigma(n) < (\beta + 1)m.$$

□ Really, since $n > m$, then $\alpha n + m < \alpha n + n = (\alpha + 1)n$; on the other hand, $\alpha n + m > \alpha m + m = (\alpha + 1)m$. □

Moreover, the following proposition, useful for a search of multiple amicable pairs, holds:

- *Let* $m, n, \alpha, \beta, a \in \mathbb{N}$, $gcd(a, m) = gcd(a, n) = 1$ *and* $\frac{\sigma(a)}{a} = \frac{m+\alpha n}{\sigma(m)} = \frac{n+\beta m}{\sigma(n)}$*; then* (am, an) *is an* (α, β)*-multiple amicable pair.*

□ It can be checked by simple computations. □

It is known that

- *in an* (α, β)*-multiple amicable pair* (m, n)*, the smaller member* m *cannot have just one distinct prime factor, and if it has precisely two prime factors, then* $\alpha = 1$ *and* m *is even.*

Quasi-amicable and augmented amicable numbers

5.3.7. *Betrothed numbers* (or *quasi-amicable numbers* or *reduced amicable numbers*) are two positive integers such that the sum of the proper divisors of either number is one more than the value of the other number. One can state also that the pair (m, n) forms a quasi-amicable pair if m is the sum of non-trivial divisors (e.g., all positive divisors without 1 and the number itself) of n, and n is the sum of non-trivial divisors of m.

In other words, the pair (m, n) is a pair of quasi-amicable numbers if

$$m = s(m) - 1 \text{ and } m = s(n) - 1.$$

An equivalent condition is

$$\sigma(m) = \sigma(n) = m + n + 1.$$

For example, the pair (48, 75) is quasi-amicable since $\sigma(48) = \sigma(75) = 124 = 48 + 75 + 1$.

Augmented amicable numbers (or *reduced amicable numbers*) are two positive integers such that the sum of the proper divisors of either number is one less than the value of the other number.

In other words, the pair (m, n) is a pair of augmented amicable numbers if

$$\sigma(m) = \sigma(n) = m + n - 1.$$

For example, the pair (6160, 11697) is augmented amicable since $\sigma(6160) = \sigma(11697) = 17856 = 6160 + 11697 - 1$.

The first few pairs of quasi-amicable numbers are (48, 75), (140, 195), (1050, 1925), (1575, 1648), (2024, 2295), (5775, 6128), (8892, 16587), (9504, 20735), (62744, 75495), (186615, 206504),... (see sequence A005276 in the OEIS; see also A003502 and A003503), in total 46 pairs with m up to 10^7.

The first few pairs of augmented amicable numbers are (6160, 11697), (12220, 16005), (23500, 28917), (68908, 76245), (249424, 339825), (425500, 570405), (434784, 871585), (649990, 697851), (660825, 678376), (1017856, 1340865),... (see sequence A281265 in the OEIS), in total 36 pairs with m up to 10^7.

5.3.8. All known pairs of quasi-amicable numbers as well as augmented amicable numbers have opposite parity.

By the definition of quasi-amicable pair, one can state that

- *if* (m, n) *is a quasi-amicable pair of the same parity, then each of its member should be a square or twice a square.*

Making use of this fact, Hagis and Lord (1977) performed a search for quasi-amicable pairs of the same parity in the range 10^7–10^{10}. None were found. At present, it is checked that

- *any pair of quasi-amicable (or augmented amicable) numbers of the same parity must exceed* 10^{13}.

Hagis and Lord also obtained the following interesting result:

- *If* (m, n) *is a quasi-amicable pair with gcd*$(m, n) = 1$, *then* m *and* n *each exceeds* 10^{30} *and* mn *has at least four distinct prime factors; moreover,* mn *has at least* 21 *distinct prime factors if it is odd.*

So, it is natural to conjecture that

- *there are no quasi-amicable pairs (or augmented amicable pairs) with the same parity.*

On the other hand, there exists a conjecture [Yan96] that

- *there are infinitely many quasi-amicable pairs and augmented amicable pairs.*

5.3.9. Let $A(x)$ be the number of amicable pairs, $A'(x)$ be the number of quasi-amicable pairs, and $A''(x)$ be the number of augmented amicable pairs not exceeding a real positive number x. The numerical analysis allows to conjecture (Cohen, 1970; [Yan96]) that

- *there exist positive constants β, β', and β'' such that*

$$\log A(x) \sim \beta \log x, \ \log A'(x) \sim \beta' \log x, \ \log A''(x) \sim \beta'' \log x.$$

For references and some additional information, see, for example, [CGH95], [HaLo77], [Yan96], [Cohe70], [Weis22], [Wiki22], and [Sloa22].

Exercises

1. Prove that the definition of amicable triple (l, m, n) can be reformulated as follows: $s(l) = m + n$, $s(m) = l + n$, $s(n) = l + m$, where $s(n) = \sigma(n) - n$. Check that the triple $(2^2 \cdot 3^2 \cdot 5 \cdot 11, 2^5 \cdot 3^2 \cdot 7, 2^2 \cdot 3^2 \cdot 71)$ is amicable.
2. Prove that the abundancy $\frac{\sigma(n)}{n}$ of n can be expressed as $\sigma_{-1}(n)$, where σ_x denotes a divisor function with $\sigma_x(n)$ equal to the sum of the xth powers of the divisors of n. Find the abundancy n for $n = 1, 2, 3, \dots, 10$.
3. Check that a friendly pair $(24, 91963648)$ has abundancy $2,5$.
4. Prove that the harmonic mean of all divisors of n is $\frac{\tau(n)n}{\sigma(n)}$.
5. Check that the abundancy of any perfect number is equal to 2. Prove that we have at least 1275 friendly pairs with common abundancy 2.

6. Check that the numbers 13 and 17 are solitary.
7. Check that the pairs (48, 75), (140, 195), and (1050, 1925) are quasi-amicable (see sequences A005276, A003502, and A003503 in the OEIS; see also A003502 and A003503).
8. Check that the pairs (6160, 11697), (12220, 16005), and (23500, 28917) are augmented (see sequence A281265 in the OEIS).

5.4. Sociable Numbers

Basic definitions

5.4.1. A positive divisor of a positive integer n which is different from n is called a *proper divisor* (or *aliquot part*) of n. The sum $s(n) = \sum_{d|n,\ d\neq n} d$, $n \in \mathbb{N}$, of all proper divisors of n is called *restricted divisor function* (or *aliquot sum function* or just *aliquot sum*) of n.

By definition, $s(n) = \sigma(n) - n$, where $\sigma(n) = \sum_{d|n} d$ is the *sum of divisors function* (or *sigma function*): the sum of positive integer divisors of a positive integer n.

Sociable numbers are defined as positive integers whose aliquot sums form a cyclic sequence that begins and ends with the same number. They are generalizations of the concepts of amicable numbers and perfect numbers.

Formally, a *k-tuple of sociable numbers* (or *amicable k-cycle* or *sociable k-cycle* or *aliquot k-cycle*) is formed by k positive integers $(x_1, x_2, \ldots, x_k)$, related in such a way that

$$s(x_1) = x_2,\ s(x_2) = x_3, \ldots, s(x_{k-1}) = x_k,\ s(x_k) = x_1.$$

By definition, for $k = 2$, we get an amicable pair, while for $k = 1$—a perfect number.

In terms of the sigma function, a *k-tuple of sociable numbers* is formed by k positive integers $(x_1, x_2, \ldots, x_k)$ such that

$$\sigma(x_1) = x_1 + x_2,\ \sigma(x_2) = x_2 + x_3, \ldots, \sigma(x_{k-1}) = x_k,$$
$$\sigma(x_k) = x_k + x_1.$$

On the other hand, for a given positive integer n, we define the *aliquot sequence* of n as

$$s^0(n) = n, s^1(n) = s(n), s^2(n) = s(s(n)), \ldots, s^k(n) = (s^{k-1}(n)), \ldots.$$

Then, for any perfect number n, we get the constant sequence $n, n, n, n, \ldots$; for any amicable pair (m, n), we get the sequence $m, n, m, n, \ldots$; for any k-tuple of sociable numbers, $(x_1, x_2, \ldots, x_k)$, we get the sequence $x_1, x_2, \ldots, x_k, x_1, x_2, \ldots, x_k, \ldots$.

Each number is the sum of the proper factors of the preceding number, i.e., the sum excludes the preceding number itself. For the sequence to be *sociable*, the sequence must be cyclic and return to its starting point. The *period of the social sequence* or *order of the set of sociable numbers* is the number of elements in this cycle.

So, any perfect number forms an aliquot sequence of period 1, i.e., a sociable number of order 1. A pair of amicable numbers constitutes an aliquot sequence of period 2, i.e., a set of sociable numbers of order 2. A k-tuple of sociable numbers forms an aliquot sequence of period k, $k \geq 3$, i.e., a set of sociable numbers of order k.

For instance, the number 6 gives an example of amicable 1-cycle: $s(6) = 6$. The pair $(220, 284)$ forms an amicable 2-cycle: $s(220) = 284$ and $s(s(220)) = s(284) = 220$. There are no known amicable 3-cycles.

The quadruple $(1264460, 1547860, 17276361305184)$ gives an example of a sociable 4-cycle. In fact, the sum $s(1264460)$ of the proper divisors of $1264460 = 2^2 \cdot 5 \cdot 17 \cdot 3719$ is

$$1 + 2 + 4 + 5 + 10 + 17 + 20 + 34 + 68 + 85 + 170 + 340$$
$$+ 3719 + 7438 + 14876 + 18595 + 37190 + 63223 + 74380 + 126446$$
$$+ 252892 + 316115 + 632230 = 1547860;$$

the sum $s(1547860)$ of the proper divisors of $1547860 = 2^2 \cdot 5 \cdot 193 \cdot 401$ is

$$1 + 2 + 4 + 5 + 10 + 20 + 193 + 386 + 401 + 772 + 802$$
$$+ 965 + 1604 + 1930 + 2005 + 3860 + 4010 + 8020 + 77393 + 154786$$
$$+ 309572 + 386965 + 773930 = 1727636;$$

the sum $s(1727636)$ of the proper divisors of $1727636 = 2^2 \cdot 521 \cdot 829$ is

$$1 + 2 + 4 + 521 + 829 + 1042 + 1658 + 2084 + 3316$$
$$+ 431909 + 863818 = 1305184;$$

lastly, the sum $s(1305184)$ of the proper divisors of $1305184 = 2^5 \cdot 40787$ is

$$1 + 2 + 4 + 8 + 16 + 32 + 40787 + 81574 + 163148 + 326296$$
$$+ 652592 = 1264460.$$

The 5-tuple (12496, 14288, 15472, 14536, 14264) is an example of sociable 5-cycle (sequence A072891 in the OEIS).

The only known 28-cycle is (14316, 19116, 31704, 47616, 83328, 177792, 295488, 629072, 589786, 294896, 358336, 418904, 366556, 274924, 275444, 243760, 376736, 381028, 285778, 152990, 122410, 97946, 48976, 45946, 22976, 22744, 19916, 17716) (sequence A072890 in the OEIS).

These two sequences provide the only sociable numbers of order $k \geq 3$ below one million.

Moreover, only these two groups of sociable numbers of orders 5 and 28, discovered and named by Poulet in 1918, were known prior to 1970. In 1970, Cohen discovered nine groups of order 4.

The first few known sociable numbers of order $k \geq 3$, more exactly, the smallest members of known sociable cycles, are 12496, 14316, 1264460, 2115324, 2784580, 4938136, 7169104, 18048976, 18656380, 28158165, 46722700, 81128632, 174277820, 209524210, 330003580, ... (sequence A003416 in the OEIS); they have orders 5, 28, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, ... (sequence A052470 in the OEIS).

The list of all known sociable numbers, represented in increasing order, starts from 12496, 14264, 14288, 14316, 14536, 15472, 17716, 19116, 19916, 22744, 22976, 31704, 45946, 47616, 48976, ... (sequence A003416 in the OEIS).

The following table summarizes the smallest members of known social cycles of order $k \geq 4$ as well as the number of such cycles known.

Order	Number	Smallest element
4	5398	1264460, 2115324, 2784580, 4938136, 7169104, 18048976, ...
5	1	12496
6	5	21548919483, 90632826380, 1771417411016, 3524434872392, 4773123705616
8	4	1095447416, 1276254780
9	1	805984760
28	1	14316

As of 2021, excluding perfect (51) and amicable ($> 10^9$) numbers, a total of > 5400 sociable cycles are known.

Properties of sociable numbers

5.4.2. At present, sociable cycles with length 3 are known. Numerical search allows us to state that

- *in any sociable triple* (x, y, z), $x < y < z$, *the smallest member* x *should be greater than* $5 \cdot 10^7$.

However, it is conjectured that

- *for* k *equal to* 3 *modulo* 4, *there exist no sociable* k*-cycles.*

In particular, there exist no cycles of length $3, 7, 11, 15, 19, 23, 27, 31, 35, 39, \ldots$.

Similar to amicable pairs, many sociable cycles $(x_1, \ldots, x_k)$ have the *cycle sums* $x_1 + \cdots + x_k$ divisible by 10. It is true for the 4-cycle $(1264460, 1547860, 17276361305184)$ as well as for the 28-cycle (14316, 19116, 31704, 47616, 83328, 177792, 295488, 629072, 589786, 294896, 358336, 418904, 366556, 274924, 275444, 243760, 376736, 381028, 285778, 152990, 122410, 97946, 48976, 45946, 22976, 22744, 19916, 17716) but not for the 5-cycle (12496, 14288, 15472, 14536, 14264).

Up to the known $\geq$ 1590 sociable k-cycles, $k \geq 3$, 96.1% of the sociable cycles satisfy this condition (up to the first 10 sociable cycles 40%; up to the first 100 sociable number cycles 77%; up to the first 500 sociable number cycles 92%; and up to the first 1000 sociable number cycles 94.9%).

It is conjectured that

- *as the number of sociable cycles with length greater than* 2 *approaches infinity, the percentage of the cycle sums divisible by* 10 *approaches* 100%.

5.4.3. Let $A'''(x)$ be the number of sociable k-cycles not exceeding a real positive number x. The numerical analysis allows us to conjecture [Yan96] that

- *there exists a positive constant* β''' *such that* $\log A'''(x) \sim \beta''' \log x$.

On the behavior of aliquot sequences

5.4.4. As we discussed before, any sociable number results in a periodic aliquot sequence called *sociable sequence* (or *sociable chain*). If the period of the sociable chain is 1, we get a perfect number. If the period is 2, the two numbers form an amicable pair. In general, if the period is $k \geq 3$, the obtained numbers are called *sociable of order k*.

For example, 1264460 (as well as 1547860, 1727636, and 1305184) is a sociable number of order 4 since its aliquot sequence is 1264460, 1547860, 1727636, 1305184, 1264460, ...

However, there exist aliquot sequences of other forms.

Many aliquot sequences terminate at 0. For example, the aliquot sequence of 10 is 10, 8, 7, 1, 0 because $s(10) = 5 + 2 + 1 = 8$, $s(8) = 4 + 2 + 1 = 7$, $s(7) = 1$, $s(1) = 0$. The aliquot sequence of 12 is 12, 16, 15, 9, 4, 3, 1, 0. The aliquot sequence of 840 (sequence A045477 in the OEIS), starting with 840, 2040, 4440, 9240, 25320, 51000, 117480, 271320, 765480, 1531320, . . . reaches 0 at the 748th term.

All such sequences necessarily end with a prime number (since the only n for which $s(n) = 1$ are primes) followed by 1 (since the only proper divisor of a prime is 1), followed by 0 (since 1 has no proper divisors).

The first few numbers whose aliquot sequence terminates at 0 are 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, . . . (sequence A080907 in the OEIS).

However, there are a variety of ways in which an aliquot sequence might not terminate.

For perfect, amicable, and sociable numbers, their aliquot sequences are cyclic, so terminate in a constant (in fact, in a perfect number) or in a cycle with length ≥ 2.

So, the numbers whose aliquot sequence is a constant sequence are the perfect numbers 6, 28, 496, 8128, 33550336, 8589869056, 137438691328, $2305843008139952128, \ldots$ (sequence A000396 in the OEIS), while numbers whose aliquot sequence terminates in a cycle with length at least 2 are 220, 284, 562, 1064, 1184, 1188, 1210, 1308, 1336, 1380, 1420, 1490, 1604, 1690, $1692, \ldots$ (sequence A121507 in the OEIS).

Some numbers have an aliquot sequence which is eventually periodic, but the number itself is not perfect, amicable, or sociable. For instance, the aliquot sequence of 95 is 95, 25, 6, 6, 6, $6, \ldots$. Numbers such as 95 that are not perfect but have an eventually repeating aliquot sequence of period 1 are called *aspiring numbers.* The first few aspiring numbers are 25, 95, 119, 143, 417, 445, 565, 608, 650, 652, 675, 685, 783, 790, $909, \ldots$ (sequence A063769 in the OEIS). There are many numbers whose aliquot sequences have not yet been completely computed, so this sequence is not fully known. In particular, 276 may, perhaps, be an element of this sequence, although this is very unlikely.

Numbers whose aliquot sequences are not known to be finite or eventually periodic are 276, 306, 396, 552, 564, 660, 696, 780, 828, 888, 966, 996, 1074, 1086, $1098, \ldots$ (sequence A131884 in the OEIS).

The following list indicates the termination's number of the aliquot sequence starting at $n = 1, 2, 3, \ldots$: 1, 2, 3, 3, 5, 6, 7, 7, 3, 7, 11, 3, 13, 7, $3, \ldots$ (sequence A115350 in the OEIS). Here, $a(n)$ gives the prime number if the sequence terminates in a prime followed by 1 and 0 (as an exception, $a(1) = 1$), $a(n)$ give a perfect number if the sequence terminates in a perfect number, $a(n)$ gives the smallest number of the cycle if the sequence terminates in an aliquot cycle, $a(n) = 0$ if the sequence is *open ended.* So far, 276 is the smallest number for which the termination of the aliquot sequence is not known. The lengths of the aliquot sequences that start at $n = 1, 2, 3, \ldots$ are 1, 2, 2, 3, 2, 1, 2, 3, 4, 4, 2, 7, 2, 5, 5, ..., respectively (sequence A044050 in the OEIS).

As of 2015, there were 898 positive integers less than 10^5 whose aliquot sequences have not been fully determined and 9,190 such integers less than 10^6.

It is an open question whether all numbers end up at either a sociable number (including perfect and amicable numbers) or at a prime (and hence 1) or, equivalently, whether there exist numbers whose aliquot sequence never terminates and hence grows without bound.

The *Catalan's conjecture* states that

- *every aliquot sequence terminates in a prime number followed by* 1*, a perfect number, a friendly pair, or an aliquot cycle.*

The alternative would be that a number exists whose aliquot sequence is infinite yet never repeats. Any one of the many numbers whose aliquot sequences have not been fully determined might be such a number.

Generalizations of sociable numbers

5.4.5. Like sociable numbers, *quasi-sociable numbers* (or *reduced sociable numbers*) are positive integers whose aliquot sums minus one form a cyclic sequence that begins and ends with the same number. They are generalizations of the concepts of *quasi-amicable numbers* and *quasi-perfect numbers.*

Formally, a *k-tuple of quasi-sociable numbers* is formed by k positive integers $(x_1, x_2, \ldots, x_k)$, related in such a way that

$$s(x_1) - 1 = x_2,\ s(x_2) - 1 = x_3, \ldots, s(x_{k-1}) - 1 = x_k,\ s(x_k) - 1 = x_1.$$

By definition, for $k = 2$, we get a quasi-amicable pair, while for $k = 1$, a quasi-perfect number.

In terms of the sigma function, a *k-tuple of quasi-sociable numbers* is formed by k positive integers $(x_1, x_2, \ldots, x_k)$ such that

$$\sigma(x_1) = x_1 + x_2 + 1,\ \sigma(x_2) = x_2 + x_3 + 1,\ \ldots, \sigma(x_{k-1}) = x_{k-1} + x_k + 1,\ \sigma(x_k) = x_k + x_1 + 1.$$

On the other hand, for a given positive integer n, we define the *quasi-aliquot sequence* (or *quasi-sociable sequence* or *reduced aliquot sequence* or *quasi-sociable chain*) of n as

$$\overline{s}^0(n) = n, \overline{s}^1(n) = \overline{s}(n), \overline{s}^2(n) = \overline{s}(\overline{s}(n)), \dots, \overline{s}^k(n) = \overline{s}(\overline{s}^{k-1}(n)), \dots,$$

where $\overline{s}(n) = \sum_{d|n,\ d\neq 1,\, d\neq n} d = s(n) - 1 = \sigma(n) - n - 1$ is the sum of non-trivial divisors of a positive integer n. Then, a number n is called a *quasi-sociable number of order k* if its quasi-aliquot sequence is cyclic with period k, $k \in \mathbb{N}$.

The first quasi-sociable sequence was discovered by M. Dickerman in 1997. It has period 8: 1215571544, 1270824975, 1467511664, 1512587175, 1530808335, 1579407344, 1638031815, 1727239544, 1215571544, ... (sequence A309227 in the OEIS).

This is the only one known quasi-sociable chain, and the second quasi-sociable chain (if exists) must have all numbers $> 10^{12}$.

5.4.6. Like aliquot sequences, quasi-aliquot sequences can have different structures.

Most quasi-aliquot sequences terminate at 0, all such sequences necessarily end with either a prime number followed by 0 or 1 followed by 0. For example, the quasi-aliquot sequence of 36 is 36, 54, 65, 18, 20, 21, 10, 7, 0. Of course, only the sequence of 1 can reach 1 since $\sigma(n) - n - 1$ is never equal to 1. Although $\sigma(1) - 1 - 1 = -1$, we change it to 0; so, the quasi-aliquot sequence for 1 has the form 1, 0.

It is widely believed that

- *every quasi-aliquot sequence ends in one of these three ways:* 0*, a quasi-amicable pair, or a quasi-sociable cycle.*

It is also widely believed that

- *almost all positive integers have quasi-aliquot sequences that terminate at* 0*.*

5.4.7. Y. Kohmoto has considered a generalization of the sociable numbers defined according to the *generalized aliquot sequence*

$$a(n) = \frac{\sigma(a(n-1))}{m},\ m \in \mathbb{N}.$$

Multiply perfect numbers (in fact, m-perfect numbers) are fixed points of this mapping since if $a(n) = a(n-1)$, then $ma(n) = \sigma(a(n))$, which is the definition of an m-perfect number.

If the sequence $a(n)$ becomes cyclic after $k > 1$ terms, it is called a $\frac{1}{m}$*-sociable number of order* k.

It is easy to prove that

- *the numbers* $2^{q-1}M_p$ *and* $2^{p-1}M_q$*, where* M_p *and* M_q *are distinct Mersenne primes, are* $\frac{1}{2}$*-sociable numbers of order* 2.

□ In fact, if M_p and M_q are distinct Mersenne primes, then

$$\frac{1}{2}\sigma(2^{q-1}M_p) = \frac{1}{2}(2^q - 1)2^p = 2^{p-1}M_q, \ \frac{1}{2}\sigma(2^{p-1}M_q) = 2^{q-1}M_p,$$

so $2^{q-1}M_p$ and $2^{p-1}M_q$ are $\frac{1}{2}$-sociable numbers of order 2. □

The following table summarizes the smallest members of the generalized $\frac{1}{m}$-aliquot sequences of order k found by Kohmoto.

m	k	Starting numbers
3	2	2096640, 422688000
4	12	3396556800

For some additional information, see, for example, [CGH95], [HaLo77], [Yan96], [Cohe70], [Deza21], [Yan96], [Wiki22], [Sloa22], and [Weis22].

Exercises

1. Check that the numbers 1264460, 1547860, 1727636, and 1305184 form a sociable quadruple.
2. Construct the aliquot sequences for the numbers $n = 1, 2, 3, \dots, 10, 25, 28, 220, 496, 12496, 14316$. What can be said about the terminated numbers of these sequences? Can they be perfect numbers?
3. Construct the quasi-aliquot sequences for the numbers $n = 1, 2, 3, \dots,$ 10, 25, 28, 220, 496, 12496, 14316. What can be said about the terminated numbers of these sequences? Can they be perfect numbers?

4. Prove that numbers $(7, 127)$ are $\frac{1}{2}$-sociable. What can be said about numbers $(3, 31)$?
5. Prove that the numbers $(2096640, 422688000)$ are $\frac{1}{3}$-sociable.

5.5. Search for Numbers Under Consideration

5.5.1. In the theory of perfect, amicable, and sociable numbers, there exist three classical groups of methods for finding all these three kind of special numbers. There are three essentially different types of methods of such generation, namely the exhaustive numerical searching methods, the algebraic assumption methods, and the algebraic constructive methods (for more information, see, for example, a monograph by S. Y. Yan [Yan96].

Methods of the first type are directly based on numerical calculations of values of sigma function.

For example, if $\sigma(N) = 2N$, we call the number n perfect. Similarly, if $\sigma(N) = kN$, $k \in \mathbb{N}$, one obtains a multiperfect number; other variants lead to quasi-perfect, almost perfect, superperfect numbers, etc.

If $\sigma(N) = \sigma(M) = N + M$, then numbers M and N form an amicable pair (M, N). On the other hand, if $\sigma(m_1) + \sigma(m_2) + \cdots + \sigma(m_k) = m_1 + m_2 + \cdots + m_k$, then numbers $(m_1, m_2, \ldots, m_k)$ from an amicable k-tuple, while if

$$\sigma(m_1) - m_1 = m_2, \sigma(m_2) - m_2 = m_3, \ldots, \sigma(m_{k-1}) - m_{k-1} = m_k, \sigma(m_k) - m_k = m_k,$$

we get an aliquot (sociable) k-cycle; there exist also quasi-amicable, augmented amicable, multiply amicable numbers, and other similar classes of special numbers.

In the second type of methods, an assumption is made about the prime structure of considered numbers. For example, for $k = 1, 2, 3, \ldots$, if $2^k - 1$ is a prime, then $N = 2^{k-1}(2^k - 1)$ is an even perfect number. On the other hand, the Thābit's rule states that for a given $n = 1, 2, 3, \ldots$, if p, q, and r are distinct primes of a special form, then the numbers $M = 2^n \cdot p \cdot q$ and $N = 2^n \cdot r$ form an amicable pair (M, N). Similar rules exist for some types of tuples of length $k \geq 3$.

In the third type of methods, new elements of considered set of special numbers are constructed from a given *mother* (or *breeder*) element of the same set. For example, the Borho's rule states that if an amicable pair $A = a \cdot u$, $B = a \cdot s$ is given, where s is prime, $(a, us) = 1$, $p = u + s + 1$ is prime, and a is not divisible by p, then the pair $(M = A \cdot p^n \cdot q_1, N = a \cdot p^n \cdot q_2)$ is an amicable pair for each $n = 1, 2, 3, \ldots$ such that both $q_1 = (u + 1) \cdot p^n - 1$ and $q_2 = (u + 1) \cdot (s + 1) \cdot p^n - 1$ are primes. Several similar approaches for k-tuples with $k \geq 3$ are considered in the last part of this section.

In this section, we present main facts concerning the historical and contemporary aspects of the search of some classes of numbers relative to perfect and amicable numbers.

Numerical methods for analogue of perfect numbers

The numerical methods are the simplest methods in which the computation is directly based on the calculation of the sigma function.

5.5.2. Recall that a positive integer n is k-perfect if $\sigma(n) = kn$, $k \in \mathbb{N}$. So, the determination of where n is k-perfect can be done by just checking the sigma value of n.

Algorithm for searching k-perfect numbers, $3 \leq k \leq 10$, in the interval $[A, B]$

- For n from A to B, find

$$\sigma(n) = \sigma(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+1} - 1}{p_s - 1}.$$

- For k from 3 to 10, if $\sigma(n) = kn$, then n is k-perfect.

Note that most computer algebra systems (Mathematica, Marple etc.) have a standard function to calculate $\sigma(n)$.

In the following, some results for n up to 10^{11} are given. The largest known value of k is 8.

3-perfect numbers	4-perfect numbers	5-perfect numbers
120	30240	14182439040
672	32760	
523776		

5.5.3. A positive integer is perfect, quasi-perfect, or almost perfect if $\sigma(n) = 2n$, $\sigma(n) = 2n + 1$, or $\sigma(n) = 2n - 1$, respectively. So, the determination of where n is perfect, quasi-perfect, or almost perfect can be done by just checking the sigma value of n.

Algorithm for searching all perfect, quasi-perfect, or almost perfect numbers in the interval $[A, B]$

- For n from A to B, find

$$\sigma(n) = \sigma(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+1} - 1}{p_s - 1}.$$

- If $\sigma(n) = 2n - 1$, then n is almost perfect.
- If $\sigma(n) = 2n$, then n is perfect.
- If $\sigma(n) = 2n + 1$, then n is quasi-perfect.

5.5.4. A positive integer is superperfect, quasi-superperfect, or almost superperfect if $\sigma(\sigma(n)) = 2n$, $\sigma(\sigma(n)) = 2n + 1$, or $\sigma(\sigma(n)) = 2n - 1$, respectively. So, the determination of where n is superperfect, quasi-superperfect, or almost superperfect can be done by just checking the sigma value of $\sigma(n)$.

Algorithm for searching all superperfect, quasi-superperfect, or almost superperfect numbers in the interval $[A, B]$

- For n from A to B, find $\sigma(\sigma(n))$.
- If $\sigma(\sigma(n)) = 2n - 1$, then n is almost superperfect.
- If $\sigma(\sigma(n)) = 2n$, then n is superperfect.
- If $\sigma(\sigma(n)) = 2n + 1$, then n is quasi-superperfect.

In the following, some results are given (in fact, for the list of the first seven almost perfect, superperfect, and quasi-superperfect numbers, see [Yan96]). It turns out that there exist no quasi-perfect and almost superperfect numbers. All powers of two are almost perfect numbers, and there are no other known numbers of this type. The known quasi-perfect numbers are just the Mersenne primes, while the only known superperfect numbers are those powers of two that lead to Mersenne primes.

Almost perfect	Superperfect	Quasi-superperfect
2	2	3
4	4	7
8	16	31
16	64	127
32	4096	8191
64	65536	131071
128	262144	524287

This algorithm can be generalized to k-superperfect numbers and their analogue for $k \geq 3$. Recall that a positive integer is k-superperfect, quasi k-superperfect, or k-almost superperfect, $k \geq 3$, if $\sigma^k(n) = \sigma(\sigma(\sigma(\dots(n)))) = 2n$, $\sigma^k(n) = \sigma(\sigma(\sigma(\dots(n)))) = 2n+1$, or $\sigma^k(n) = \sigma(\sigma(\sigma(\dots(n)))) = 2n-1$, respectively. So, the determination of at which n is k-superperfect, quasi k-superperfect, or k-almost superperfect can be done by just checking the value $\sigma^k(n)$, where $\sigma^1(n) = \sigma(n)$ and $\sigma^{i+1}(n) = \sigma(\sigma^i(n))$, $i = 2, 3, \dots$, i.e., by the following simplest numerical method.

Algorithm for searching all k-superperfect, quasi k-superperfect, or k-almost superperfect numbers, $3 \leq k \leq 10$, in the interval $[A, B]$

- For n from A to B, find $\sigma(n)$ and $\sigma^2(n)$.
- For k from 3 to 10, find $\sigma^k(n)$.
- If $\sigma^k(n) = 2n - 1$, then n is almost k-superperfect.
- If $\sigma^k(n) = 2n$, then n is k-superperfect.
- If $\sigma^k(n) = 2n + 1$, then n is quasi k-superperfect.

The major computation of the above algorithms is the computation of $\sigma(n)$ which is based on the complete integer factorization of n. Since at the present time, no efficient factoring algorithm has been found, the algorithms cannot be performed in deterministic polynomial time.

Numerical methods for analogue of amicable numbers

Recall that a pair (m_1, m_2) is quasi-amicable if $\sigma(m_1) = \sigma(m_2) = m_1 + m_2 + 1$. If $\sigma(m_1) = \sigma(m_2) = m_1 + m_2 - 1$, then the pair (m_1, m_2) is an augmented amicable pair.

Algorithm for searching all quasi-amicable and augmented amicable pairs (m_1, m_2) with $m_1 < m_2$, where m_1 is in the interval $[A, B]$

- For m_1 from A to B, find

  $$m_2 = \sigma(m_1) - m_1 - 1 = \sigma(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) - p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s} - 1.$$
- If $m_2 > m_1$, find $\sigma(m_2)$.
- If $\sigma(m_2) = \sigma(m_1)$, then (m_1, m_2) is a quasi-amicable pair.
- For m_1 from A to B, find

  $$m_2 = \sigma(m_1) - m_1 + 1 = \sigma(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}) - p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s} + 1.$$
- If $m_2 > m_1$, find $\sigma(m_2)$.
- If $\sigma(m_2) = \sigma(m_1)$, then (m_1, m_2) is an augmented amicable pair.

At present, all quasi-amicable and augmented amicable pairs up to 10^7 are found.

Numerical methods for sociable numbers

Recall that k distinct positive integers $(m_1, \ldots, m_k)$ form an aliquot k-cycle (or sociable group of order k) if

$$\sigma(m_1) = m_1 + m_2,\ \sigma(m_2) = m_2 + m_3,$$

$$\sigma(m_3) = m_3 + m_4, \ldots \sigma(m_{k-1}) = m_{k-1} + m_k,\ \sigma(m_k) = m_k + m_1.$$

Similar to the algorithms for perfect and amicable numbers, one can use the following.

General numerical algorithm for aliquot k-cycles

- For m_1 from A to B, find
$$m_2 = \sigma(m_1) - m_1, m_3 = \sigma(m_1) - m_1, \dots,$$
$$m_k = \sigma(m_{k-1}) - m_{k-1}, m_{k+1} = \sigma(m_k) - m_k.$$
- If $m_{k+1} = m_1$ and $m_1 \neq m_2 \neq \cdots \neq m_k$, then $(m_1, \dots, m_k)$ is an aliquot k-cycle.

Of course, we can design this algorithm to generate all the perfect, amicable, and sociable numbers within a specified interval.

For example, for $m_2 = \sigma(m_1) - m_1$, $m_3 = \sigma(m_2) - m_2$, $m_4 = \sigma(m_3) - m_3$, $m_5 = \sigma(m_4) - m_4$, if $m_1 = m_2 = m_3 = m_4$, then m_1 is perfect; if $m_1 = m_3$ and $m_2 = m_4$, then (m_1, m_2) is amicable; if $m_5 = m_1$ and $m_1 \neq m_2 \neq m_3 \neq m_4$, then $(m_1, \dots, m_4)$ is sociable.

Compared with amicable pairs, many fewer numbers of aliquot k-cycles have been found. Poulet was the first who discovered two such cycles in 1918, one of the order 5 and the other of the order 28. Up to 1970, these were the only two known. In 1970, Choen found nine new aliquot 4-cycles. Moews and Moews have conducted several brute-force searches for aliquot cycles in the range from 1 to $6.5 \cdot 10^{10}$ and found some new cycles. Yan presented in [Yan96] a large list of sociable numbers, including 35 4-cycles, one 5-cycle, one 6-cycle, two 8-cycles, one 9-cycle, and one 28-cycle.

Most of the recent cycles have been found by numerical exhaustive methods on a computer.

Algebraic assumption methods for aliquot k-cycles

5.5.5. There exist several algebraic rules for sociable numbers. In this section, we consider some of them. In particular, we use a famous rule proposed by Borho in 1969 for aliquot 3-cycles. This is the only known rule for sociable numbers of order 3.

In fact, the *Borho's rule for aliquot* 3*-cycles* states that

- *if* $u, v \in \mathbb{N}$ *and* $u \geq v$, $2u + 1 \equiv 0(mod\ v)$, *then the numbers*

$$p = 2^v - 1,\ p_1 = \tfrac{(2^{v+1}-1)(2^u-1)+2^{u-v}(2^{u+1}-1)}{p},$$
$$p_2 = 2^v(p_1 + 2) - 1,\ p_3 = 2^v(2^{v+1} - 1) + 2^{u+1} - 1$$

are integers; if p, p_1, p_2, p_3 *are all primes, then* $(m_1, m_2, m_3) = (2^v \cdot p \cdot p_1, 2^v \cdot p_2, 2^u \cdot p_3)$ *is an aliquot* 3*-cycle.*

In the algorithm for implementation of the Borho's rule, we need to test the primality of p_1, p_2, p_3 only when $p = 2^v - 1$ is a Mersenne prime with v an odd prime (v must be odd since it divides $2u+1$) and u even (if u were also odd, we would have $2^{v+1} \equiv 1(mod\ 3)$, $2^{u+1} \equiv 1(mod\ 3)$, and so, $p_1 \equiv 0(mod\ 3)$ which would make p_1 composite as it is easy to check that $p_1 > 3$).

Borho's algorithm for searching aliquot 3-cycles with u in the interval $[A, B]$

- For a given u from A to B and for any v from A to u, if $2u + 1 \equiv 1(mod\ v)$, then find $p = 2^v - 1$.
- If p is prime, then find

$$p_1 = \frac{(2^{v+1} - 1)(2^u - 1) + 2^{u-v}(2^{u+1} - 1)}{p},$$
$$p_2 = 2^v(p_1 + 2) - 1,\ p_3 = 2^v(2^{v+1} - 1) + 2^{u+1} - 1.$$

- If p_1, p_2, p_3 are all primes, then find $m_1 = 2^v \cdot p \cdot p_1$, $m_2 = 2^v \cdot p_2$, $m_3 = 2^u \cdot p_3$.
- Indicate (m_1, m_2, m_3) as an aliquot 3-cycle.

The computational analysis shows that there are no values for $u, v \leq 10^{10}$ in the present rule which can generate any aliquot 3-cycle. As one can check (see [Yan96]), it is almost impossible to have p_1, p_2, p_3 all primes even if p is Mersenne prime and v is odd prime.

This situation allows us to state that, maybe, *there are no aliquot 3-cycles*. Such a conjecture was made, for example, by R. Guy [Guy94].

However, one can conjecture that *there exist infinitely many aliquot 3-cycles*. We have not found such cycles yet probably because at present, we have not enough computer power or we have not found other, more suitable rules for aliquot 3-cycles [Yan96].

5.5.6. It turn out that the classical Euler's method for amicable pairs of the form $(a \cdot p \cdot q, a \cdot s)$ can be generalized to aliquot $2k$-cycles. The following is such a generalization for 4-cycles, which is due to Borho (see, for example, [Yan96]):

- *If* $a_1, a_2, d_1, d_2 \in \mathbb{N}$, $a_1 a_2 = d_1 d_2$, *and*

$$p_1 = \frac{s(a_2)\sigma(a_1) + d_1\sigma(a_2)}{a_1a_2 - s(a_1)s(a_2)},\ p_2 = \frac{s(a_2)\sigma(a_1) + d_2\sigma(a_2)}{a_1a_2 - s(a_1)s(a_2)},$$
$$q_1 = \frac{s(a_1)\sigma(a_2) + d_1\sigma(a_1)}{a_1a_2 - s(a_1)s(a_2)},\ q_2 = \frac{s(a_1)\sigma(a_2) + d_2\sigma(a_1)}{a_1a_2 - s(a_1)s(a_2)},$$
$$r = \frac{s(a_1p_1p_2)}{a_1},\ t = \frac{s(a_2q_1q_2)}{a_2}$$

  are all integers and primes, $p_1 \neq p_2$, $q_1 \neq q_2$, *and* $gcd(p_1, a_1) = gcd(p_2, a_1) = gcd(r, a_1) = gcd(q_1, a_2) = gcd(q_2, a_2) = gcd(t, a_2) = 1$, *then*

$$(m_1, m_2, m_3, m_4) = (a_1 \cdot p_1 \cdot p_2, a_1 \cdot r, a_2 \cdot q_1 \cdot q_2, a_2 \cdot t)$$

  is an aliquot 4*-cycle.*

Algorithm for searching of aliquot 4-cycles with a_1, a_2, d_1, d_2 in the interval $[A, B]$

- Choose a large integer R and factor R.
- Write R as a product of UV, $A \leq U, V \leq B$, in all possible ways.
- Select one of the pairs UV as a_1a_2; select another pair as d_1d_2.
- Find $S_1 = \sigma(a_1)$, $S_2 = \sigma(a_2)$, $s_1 = S_1 - a_1$, $s_2 = S_2 - a_2$, $A = a_1a_2 - s_1s_2$, $B_1 = s_2S_1 + d_1S_2$, $B_2 = s_2S_1 + d_2S_2$, $B_3 = s_1S_2 + d_1S_1$, and $B_4 = s_1S_2 + d_2S_1$.

- Find $p_1 = \frac{B_1}{A}$, $p_2 = \frac{B_2}{A}$, $q_1 = \frac{B_3}{A}$, and $q_2 = \frac{B_4}{A}$.
- Find $B_5 = \sigma(a_1 p_1 p_2) - a_1 p_1 p_2$ and $B_6 = \sigma(a_2 q_1 q_2) - a_1 q_1 q_2$.
- Find $r = \frac{B_5}{a_1}$ and $t = \frac{B_6}{a_2}$.
- If $B_i \equiv 0(mod\ A)$, $i = 1, \ldots, 4$, $B_5 \equiv 0(mod\ a_1)$, and $B_6 \equiv 0(mod\ a_2)$, then
- if p_1, p_2, q_1, q_2, r, t are all primes, then
- if $gcd(p_1, a_1) = gcd(p_2, a_1) = gcd(r, a_1) = gcd(q_1, a_2) = gcd(q_2, a_2) = gcd(t, a_2) = 1$ and $p_1 \neq p_2$, $p_1 \neq q_2$, then
- find $m_1 = a_1 \cdot p_1 \cdot p_2$, $m_2 = a_1 \cdot r$, $m_3 = a_2 \cdot q_1 \cdot q_2$, $m_4 = a_2 \cdot t$.
- Indicate (m_1, m_2, m_3, m_4) as an aliquot 4-cycle.

For example, the quadruple $(28158165, 29902635, 30853845, 2997155)$ has the above form with $a_1 = 3^3 \cdot 5 \cdot 7$, $d_1 = 3^2 \cdot 5 \cdot 7$, $p_1 = 83$, $p_2 = 359$, $r = 31643$, $a_2 = 3^3 \cdot 5 \cdot 11$, $d_2 = 3^4 \cdot 5 \cdot 11$, $q_1 = 79$, $q_2 = 263$, $t = 20183$.

5.5.7. From our consideration, it follows, for a proper choice of parameters (see Chapter 4 and [Yan96]), that

- *for* $u, v, \lambda \in \mathbb{N}$, $u < v$, $u < \lambda < 2v - u$, *if*

$$p = 2^v + 2^u - 1,\ q = (2^{v-u} + 1)(2^{2v-\lambda} + 2^v - 1) - 2^{2v-u-\lambda},$$
$$r = (2^{v-u} + 1)(2^v - 1) + 2^{2v-u},$$
$$s = (2^{v-u} + 1)(2^v + 2^\lambda) - 1,\ t = (2^{v-u} + 1)(2^v + 2^{2v-\lambda} p) - 1,$$
$$m = (2^{v-u} + 1)(2^{v+1} - 1)(2^{v-\lambda} + 1)(r + 1) - qr,$$
$$n = (2^{v+1} - 1)(s + 1)(t = 1)2^{-v} - st$$

are all primes and $p \neq q$, $p \neq r$, $p \neq m$, $q \neq r$, $s \neq t$, *then*

$$(m_1, m_2, m_3, m_4) = (2^v \cdot p \cdot q \cdot r, 2^v \cdot p \cdot m, 2^v \cdot s \cdot t, 2^v \cdot n)$$

is an aliquot 4*-cycle.*

Algorithm for searching 4-cycles with $\boldsymbol{u, v, l}$ in the interval $[\boldsymbol{A, B}]$

- For u from A to B, for v from A to B, and for l from A to B, if $u < v$, $u < l$, and $l < 2v - u$, then find

$$\begin{aligned} p &= 2^v + 2^u - 1,\ q = (2^{v-u} + 1)(2^{2v-\lambda} + 2^v - 1) - 2^{2v-u-\lambda},\\ r &= (2^{v-u} + 1)(2^v - 1) + 2^{2v-u},\\ s &= (2^{v-u} + 1)(2^v + 2^\lambda) - 1,\ t = (2^{v-u} + 1)(2^v + 2^{2v-\lambda}p) - 1,\\ m &= (2^{v-u} + 1)(2^{v+1} - 1)(2^{v-\lambda} + 1)(r + 1) - qr,\\ n &= (2^{v+1} - 1)(s + 1)(t = 1)2^{-v} - st. \end{aligned}$$

- If p, q, r, s, t, m, n are all primes and $p \neq q$, $p \neq r$, $p \neq m$, $q \neq r$, and $s \neq t$, then find

$$m_1 = 2^v \cdot p \cdot q \cdot r, m_2 = 2^v \cdot p \cdot m, m_3 = 2^v \cdot s \cdot t, m_4 = 2^v \cdot n.$$

- Indicate (m_1, m_2, m_3, m_4) as an aliquot 4-cycle.

The considered algebraic methods for aliquot 4-cycles can be extended to higher orders $2k > 4$.

Algebraic constructive methods for amicable $\boldsymbol{k}$-tuples

5.5.8. Recall that k positive integers $m_1, \ldots, m_k$ form an amicable k-tuple if

$$\sigma(m_1) = \sigma(m_2) = \ldots = \sigma(m_k) = m_1 + m_2 + \cdots + m_k.$$

In [Yan96], Yan proposed two constructive methods for amicable k-tuples. First one, for amicable triples, is based on the ideas by Dickson, who systematically studied amicable triples, proposed for them two Thābit-like rules, and found several examples ([Dick13a]).

The second pure constructive method can be used for any amicable k-tuples. It states that

- *if there are positive integers* $m_1, \ldots, m_k$ *such that*

  $$\sigma(m_1) = \sigma(m_2) = \cdots = \sigma(m_k) \quad \textit{and} \quad \sigma(m_1) \neq m_1 + \cdots + m_k,$$

  and if there exists another positive integer a *such that*

  $$gcd(a, m_1) = \cdots = gcd(a, m_k) \quad \textit{and} \quad \frac{\sigma(a)}{a} = \frac{m_1 + \cdots + m_k}{\sigma(m_1)},$$

  then $(a \cdot m_1, a \cdot m_2, \ldots, a \cdot m_k)$ *is an amicable* k*-tuple.*

□ By definition, $(a \cdot m_1, a \cdot m_2, \ldots, a \cdot m_k)$ is an amicable k-tuple if it satisfies the conditions

$$\sigma(am_1) = \sigma(am_2) = \cdots = \sigma(am_k), \quad \text{and} \quad \sigma(am_1) = a(m_1 + \cdots + m_k).$$

We selected k positive integers $m_1, \ldots, m_k$ such that $\sigma(m_1) = \sigma(m_2) = \cdots = \sigma(m_k)$. If another positive integer a exists such that $gcd(a, m_1) = \cdots = gcd(a, m_k)$, then the first condition holds: $\sigma(am_1) = \sigma(am_2) = \cdots = \sigma(am_k)$. Furthermore, if $\frac{\sigma(a)}{a} = \frac{m_1 + \cdots + m_k}{\sigma(m_1)}$, then $\sigma(a)\sigma(m_1) = a(m_1 + \cdots + m_k)$, and the second condition holds. So, we get that $(a \cdot m_1, a \cdot m_2, \ldots, a \cdot m_k)$ is an amicable k-tuple. □

Algorithm for searching amicable *k*-tuples with *a* in the interval $[A, B]$

- Find k positive integers $m_1, \ldots, m_k$ satisfying

  $$\sigma(m_1) = \sigma(m_2) = \cdots = \sigma(m_k), \; \sigma(m_1) \neq m_1 + \cdots + m_k$$

  (one can use for it a given amicable k-tuple).
- Calculate $B = \sigma(m_1)$, $C = m_1 + \cdots + m_k$.
- For a from A to B, find $S = \sigma(a)$, $b = gcd(a, m_1)$.
- If $b = gcd(a, m_2) = \cdots = gcd(a, m_k)$ and if $SB = aC$, then find $a \cdot m_1, a \cdot m_2, \ldots, a \cdot m_k$.
- Indicate $(a \cdot m_1, a \cdot m_2, \ldots, a \cdot m_k)$ as an amicable k-tuple.

As we can see, many positive integers may have the same sigma value. For k such numbers $m_1, \ldots, m_k$, if we can find another number a such that $\sigma(am_i) = \sigma(am_j)$, $i, j = 1, 2, \ldots, k$ and $\sigma(a)\sigma(m_i) = a(m_1 + \cdots + m_k)$, we get an amicable k-tuple $(a \cdot m_1, \ldots, a \cdot m_k)$. It should be not so difficult to find such a, so the chance of finding amicable k-tuples is really large.

However, as this method is based on the calculation of the sigma function, it cannot be performed in polynomial time.

For detailed consideration of the presented and other algorithms with elements of practical computational approach, see [Yan96]; for some additional information, see also [Dick13a], [Borh69], [Wiki22], and [Sloa22].

Exercises

1. Use the algorithm of numerical method to find all perfect, almost perfect, and quasi-perfect numbers in the interval $[1, 200]$.
2. Use the algorithm of numerical method to find all superperfect, almost superperfect, and quasi-superperfect numbers in the interval $[1, 200]$.
3. Use the algorithm of numerical method to find all k-perfect numbers, $k = 1, 2, 3, 4$, in the interval $[1, 200]$.
4. Use the algorithm of numerical method to find all quasi-amicable and augmented amicable pairs in an interval $[A, B]$. Which interval are you going to consider?
5. Prove that Borho's rule for aliquot 3-cycles really gives sociable triples. Use the corresponding algorithm to prove that there are no aliquot 3-cycles in the interval $[1, 1000]$.

5.6. Open Problems

There are many open questions in the theory of sociable numbers as well as their numerous analogues. Many such questions and corresponding conjectures were considered earlier.

In this section, we collect this information and give some additional explanations and examples.

Existence, finiteness, and infiniteness

5.6.1. The main question of the theory of any class of special numbers is a question about the cardinality of corresponding number set.

For example, it is well known that there are infinitely many prime numbers as well as, for example, prime numbers of the form $6k-1$. But the question about the infiniteness of the set of primes of the form 2^k-1 (in fact, Mersenne primes $M_p = 2^p - 1$) is open. It leads to the famous *Mersenne conjecture* which states that

- *there are infinitely many Mersenne primes.*

On the other hand, the study of the behavior of the set of primes of the form 2^k+1 (in fact, Fermat primes $F_n = 2^{2^n}+1$) leads to the *Fermat conjecture*, which states that

- *the set of Fermat primes is finite.*

Unfortunately, both questions have no answer at present.

If the Mersenne conjecture is true, then we can answer "yes" to the main question of the theory of perfect numbers:

- *Are there infinitely many even perfect numbers?*

But probably, the answer to the question

- *Are there odd perfect numbers?*

is "no."

As for amicable numbers, we also do not know,

- *If there are infinitely many amicable pairs?*

5.6.2. Similar questions arise in the study of other number sets connected with perfect and amicable numbers.

In fact, there exist the following conjectures about cardinalities of the sets under our consideration:

- there are infinitely many sociable numbers of order k, $k \geq 4$; more exactly, for any $k > 3$, there exist infinitely many aliquot k-cycles;

- there are infinitely many quasi-amicable pairs and augmented amicable pairs;
- there are infinitely many almost perfect, superperfect, and quasi-superperfect numbers;
- there are infinitely many primitive weird numbers; etc.

On the other hand, it is conjectured that

- there are no aliquot 3-cycles; in general, for any k equal to 3 modulo 4, there exist no sociable k-cycles;
- there are no quasi-amicable pairs (or augmented amicable pairs) with the same parity;
- there are no quasi-perfect and almost superperfect numbers;
- there are no $(m, 2)$-superperfect numbers for $m > 3$;
- the sets of k-perfect numbers, $k \geq 3$, are finite;
- beyond perfect numbers, all clubs of friendly numbers are finite, etc.

Catalan's conjecture

5.6.3. The *Catalan's conjecture* (sometimes called also the *Catalan–Dickson conjecture*), proposed by Catalan in 1888 and later extended by Dickson, states that

- *every aliquot sequence terminates in a prime number followed by* 1*, a perfect number, an amicable pair, or an aliquot cycle.*

The alternative would be that a number exists whose aliquot sequence is infinite. Any one of the many numbers whose aliquot sequences have not been fully determined might be such a number.

Guy and Selfridge believe that the Catalan–Dickson conjecture is false and that there exist some aliquot sequences which are unbounded above.

The aliquot sequence for n is the trajectory of n under repeated application of the map $x \to s(x)$. Up to 1000, there are 12 numbers whose full trajectories are currently unknown (see sequence A131884 in the OEIS). Five well-known hard cases are 276, 552, 564, 660, 966; they are often called the *Lehmer five* (named after D. H. Lehmer).

Seven others are: 306, 396, and 696, on the same trajectory as 276; 780, on the same trajectory as 564; 828, on the same trajectory as 660; 888, on the same trajectory as 552; and 996, on the same trajectory as 660.

Any such number, e.g., 276, may have an infinite trajectory or may reach a high apex in its aliquot sequence and then descend; in fact, the number 138 reaches a peak of 179931895322 before returning to 1.

Similar conjectures exist for generalized aliquot sequences. In particular, it is widely believed that

- *every quasi-aliquot sequence ends in one of these three ways: prime number followed by* 0*, a quasi-amicable pair, or a quasi-sociable cycle.*

Other problems

5.6.4. Let $A(x)$ be the number of amicable pairs, $A'(x)$ be the number of quasi-amicable pairs, $A''(x)$ be the number of augmented amicable pairs, and $A'''(x)$ be the number of sociable k-cycles, not exceeding a real positive number x. Numerical analysis allows us to conjecture (Cohen, 1970; [Yan96]), that

- *there exist positive constants* β, β', β'', *and* β''' *such that*

$$\log A(x) \sim \beta \log x, \ \log A'(x) \sim \beta' \log x,$$

$$\log A''(x) \sim \beta'' \log x, \ \log A'''(x) \sim \beta''' \log x.$$

5.6.5. It is conjectured also that

- *as the number of sociable cycles with length greater than* 2 *approaches infinity, the percentage of the cycle sums divisible by* 10 *approaches* 100%*.*

A similar result was obtained in Chapter 4 for amicable pairs.

For additional information, see, for example, [Cata88], [Dick13], [Yan96], [Wiki22], [Weis22], and [Sloa22].

Exercises

1. Check Catalan's conjecture for all $n = 1, 2, 3, \ldots, 30$.
2. Find a friendly group which has more than 50 members.
3. Fine a friendly group which has exactly one member.
4. Show that there are infinitely many friendly groups having exactly one member each.

References

[IrRo90], [Arno38], [Apos86], [BePa01], [BiBa70], [Bras88], [Buch09], [Chan70], [Cohn65], [Dave99], [Dede63], [DeKo18], [Dick27], [Dick05], [Ehrm67], [Eule48], [Gard89], [Gelf98], [Gill64], [GKP94], [HaWr79], [Ingh32], [Ivic85], [Kahn67], [Kerc83], [Kara83], [KaVo92], [Knut68], [Knut76], [Kobl87], [Kost82], [Lagr70], [Land09], [Lege79], [LiNi96], [Luca75], [Moto83], [Nico26], [Hogg69], [Poll74], [Prim22], [Sing00], [SlPl95], [Salo90], [Stra16], [Titc87], [Weis99], and [Wiki22].

This page intentionally left blank

Chapter 6

Zoo of Numbers

In this chapter, we collect some remarkable individual special numbers, related to perfect and amicable numbers (see [DeDe12], [Deza17], [Deza18], [Deza21], [LeLi83], [SlPl95], [Weis99], [Weis22], [Wiki22], etc.).

- **2**: the only even prime; the first Sophie Germain prime; the first untouchable number.
- **3**: the first odd prime; the first non-totient number; the first perfect totient number; the first Fermat prime, F_0; the first Mersenne prime, M_2; the only triangular Mersenne prime; according to the Pythagorean school, the number 3, which they called *triad*, is the noblest of all digits, as it is the only number to equal the sum of all the terms below it and is the only number whose sum with those below it equals the product of them and itself.
- **5**: the only known odd *untouchable number*; the first safe prime; the only prime pentagonal number; the first trapezoidal number; the second Fermat prime, F_1; the only prime, digit in which a perfect square can end; the only prime whose square is composed of only prime digits.
- **6**: the first perfect number; the first unitary perfect number; the only number that is both the sum and the product of three consecutive positive numbers; the largest of the four all-harshad numbers;

the largest known number n such that there are n integers for which all pairwise sums are perfect squares.

- **7**: the third Mersenne prime, M_3; the first double Mersenne prime; the only prime p such that $p+1$ is a perfect cube; the only prime equal to the difference of the product and the sum of the two previous primes; the biggest (besides 4 and 5) known solution of the *Brocard's problem*: to find integers n such that $n!+1$ is a perfect square; the largest known prime that is not the sum of a triangular number, a square, and a cube, all of them positive; the first Kynèa number.
- **8**: the largest Fibonacci number of the form $p+1$ or $p-1$ for a prime p; the largest composite number such that all its proper divisors plus 1 are primes.
- **9**: the only known composite number n such that both 2^n+n^2 and 2^n-n^2 are primes (in fact, the primes 431 and 593); 9 is the only positive perfect power that is one more than another positive perfect power.
- **10**: the base of the decimal numeral system; the smallest noncototient number; the sum of the first three prime numbers, of the four first positive integers, and also of the first four factorials; the smallest number whose status as a possible friendly number is unknown; the only number with the property that the sum as well as the difference of its prime divisors are primes ($2+5=7$ and $5-2=3$).
- **11**: the smallest prime repuint; the only prime ($2\cdot 3+5$) of the form $p_1\cdot p_2+p_3$, where p_1, p_2, p_3 are consecutive primes; the only prime that can be expressed ($2^3+3=3^2+2$) by two consecutive primes in the forms p^q+q and q^p+p; the largest integer that cannot be expressed as a sum of at least two distinct primes; the largest number which is not expressible as sum of two composite numbers.
- **12**: the first abundant number; the first sublime number: the number of its divisors and the sum of its divisors are both perfect numbers.
- **13**: the smallest emirp; the only prime that can divide two successive integers of the form n^2+3; the only prime sum (2^2+3^2)

of squares of two consecutive primes; the prime whose square is equal to the sum of squares of all digits in which primes end: $13^2 = 1^2 + 2^2 + 3^2 + 5^2 + 7^2 + 9^2$; the largest known Fibonacci prime with index of a Fibonacci prime; the smallest prime having exactly one representation as a sum of squares greater than one (31, its reversal, is the largest one).

- **14**: the first even non-totient number.
- **15**: the smallest Mersenne composite, M_4; the first $(2, 4)$-perfect (i.e., 4-superperfect) number; the product of two consecutive Fermat primes, 3 and 5 (thus, a regular polygon with 15 sides is constructable with compass and unmarked straightedge); the smallest number that can be factorized using Shor's quantum algorithm.
- **16**: the largest known integer n for which $2^n + 1$ (in fact, F_4) is prime; the only integer of the form $n^m = m^n$ for distinct integers n and m: $16 = 2^4 = 4^2$.
- **17**: the third Fermat prime, F_2; the only prime that is the average $(\frac{13+21}{2})$ of two consecutive Fibonacci numbers; the only prime that is the sum $(17 = 2+3+5+7)$ of four consecutive primes; the only prime of the form $p^q + q^p$, where p and q are primes: $17 = 2^3 + 3^2$; the only number n having n partitions of prime parts; the only known prime that is equal to the sum of digits of its cube: $17^3 = 4913$ and $4 + 9 + 1 + 3 = 17$.
- **18**: the first solitary number with $gcd(n, \sigma(n)) > 1$.
- **20**: the smallest primitive abundant number (abundant whose proper divisors are all deficient); the smallest non-perfect semiperfect number; the product of the number of divisors and the number of proper divisors of 20 is exactly 20.
- **21**: the first non-perfect k-hyperperfect (in fact, 2-hyperperfect) number; the sum of the divisors of the first five positive integers $(1 + (1 + 2) + (1 + 3) + (1 + 2 + 4) + (1 + 5) = 21)$.
- **23**: the smallest odd prime that is not a twin prime; the smallest odd prime to be a highly cototient number; the largest integer n such that no factor of a binomial coefficient $\binom{n}{k}$ is a perfect square; the biggest prime, besides $2, 3, 5, 7$, and 11, which is uniquely expressible as a sum of at most four squares.

- **24**: the first Erdős–Nicolas number; the first non-perfect $\mathcal{S}$-perfect number; the sum of the twin primes 11 and 13; the only integer $n > 1$ such that $\sum_{i=1}^{n} i^2$ is a perfect square: $\sum_{i=1}^{24} i^2 = 70^2$; the smallest 5-hemiperfect number.
- **25**: the third Cullen number $3 \cdot 2^3 + 1$; the first aspiring number; the smallest Fermat pseudoprime modulo 7, i.e., satisfying the congruence $7^n \equiv 7(mod\ n)$; the only perfect square of the form $k^3 - 2$.
- **26**: the smallest number that is both a non-totient and a non-cototient number; the smallest non-palindrome whose square ($26^2 = 676$) is a palindrome; the largest integer n such that the segment $[m, m + 100]$ contains n primes (it happens only for $m = 2$).
- **28**: the second perfect number; the only perfect number of the form $n^k + m^k$ with $k > 1$: $28 = 3^3 + 1^3$; the only known number which can be expressed as a sum of the first positive integers $(1 + 2+3+4+5+6+7)$, a sum of the first five primes $(2+3+5+7+11)$, and a sum of the first non-primes $(1 + 4 + 6 + 8 + 9)$.
- **29**: the only two-digit prime whose square is the sum of squares of two consecutive two-digit numbers: $29^2 = 20^2 + 21^2$; the smallest prime equal to the sum of three consecutive squares: $29 = 2^2 + 3^2 + 4^2$; the smallest multi-digit prime which on adding its reverse gives a perfect square: $29 + 92 = 11^2$; the only *non-titanic prime* (i.e., with less than 1000 decimal digits) of the form $p^p + 2$.
- **30**: the only integer n, besides $0, 3, 8, 10, 18$, and 24, such that the number of its divisors is equal to the number of integers $k, 0 < k < n$, which are coprime with n; the largest integer n such that all integers $k, 0 < k < n$, which are coprime with n, are also primes.
- **31**: the third Mersenne prime, M_5; the smallest prime that can be represented as a sum of two triangular numbers in two different ways: $31 = 21 + 10 = 28 + 3$; the smallest prime that can be represented as a sum of two triangular numbers with prime indices; there are only 31 numbers that cannot be expressed as a sum of distinct squares; $3 + 5 + 7 + 11 + \cdots + 89 = 31^2$, i.e., a sum of the first 31 odd primes is a square of prime.
- **33**: the smallest odd repdigit that is not a prime number; the largest integer which is not a sum of distinct triangular numbers.

- **36**: the smallest perfect square expressible as a sum of four consecutive primes which are also two couples of prime twins: $36 = 5 + 7 + 11 + 13$; the smallest triangular number whose sum of divisors as well as sum of its proper divisors are also triangular numbers.
- **41**: the smallest prime whose cube can be written as a sum of three cubes in two ways: $41^3 = 40^3 + 17^3 + 2^3 = 33^3 + 32^3 + 6^3$; a sum of two consecutive squares: $4^2 + 5^2$.
- **42**: the first $(2, 6)$-perfect (i.e., 6-superperfect) number; the answer to the Ultimate Question of Life, the Universe, and Everything according to the *Hitchhikers Guide to the Galaxy*; the smallest number n such that n^2 is the mean of cubed twin primes, $42^2 = \frac{11^3+13^3}{2}$.
- **46**: the biggest even number which cannot be represented as a sum of two abundant numbers.
- **48**: the first quasi-amicable (betrothed) number; the first quasi-amicable pair is (48, 75).
- **60**: the first non-perfect unitary perfect number; the first non-perfect bi-unitary perfect number.
- **65**: the only number which gives a square of prime on adding as well as subtracting its reverse from it: $65+56 = 11^2$, $65-56 = 3^2$; the only number which is the difference (3^4-2^4) of two biquadratic numbers with prime indices; $(65!)^2 + 1$ is prime.
- **67**: the smallest multi-digit prime whose square, 4489, and cube, 300763, consist of different digits.
- **70**: the first weird number (e.g., abundant but not semiperfect).
- **75**: the smallest non-prime *deficient number* whose sum as well as product of aliquot divisors is a perfect square.
- **81**: a perfect totient number; the only known square n such that $n \cdot 2^n - 1$ is a prime.
- **83**: the largest known prime that can be expressed as a sum of three positive triangular numbers in exactly one way; the smallest prime whose square 6889 is a strobogrammatic number; the only prime equal to a sum of squares of odd primes: $83 = 3^2 + 5^2 + 7^2$; the only prime of the form $p^4 + 2$, where p is a prime.

- **89**: the smallest positive integer whose square, 7921, and cube, 704969, are likewise primes upon reversal.
- **90**: the biggest known bi-unitary perfect number.
- **100**: the smallest perfect square whose summation of the differences between itself and each of its digits, where each difference is raised to the power of the corresponding digit, is equal to a prime: $101 = (100 - 1)^1 + (100 - 0)^0 + (100 - 0)^0$ is a prime.
- **101**: the smallest three-digit strobogrammatic prime; the smallest three-digit palindrome prime.
- **109**: the smallest number (coincidentally prime) that has more distinct digits than its square 11881; a strobogrammatic prime, which is equal to the square root of the strobogrammatic number 11881.
- **113**: the smallest prime which is a sum of three biquadratic numbers with prime indices: $113 = 2^4 + 2^4 + 3^4$.
- **120**: the first multiply perfect (in fact, 3-perfect) number with $k \geq 3$; a highly composite, superior highly composite, untouchable, and superabundant number.
- **121**: the only perfect square of the form $1+p+p^2+p^3+p^4$, $p \in P$: $121 = 1 + 3 + 3^3 + 3^3 + 3^4$; the only, besides 4, perfect square of the form $n^3 - 4$ ($121 = 5^3 - 4$).
- **127**: the fourth Mersenne prime, M_7; the exponent for the 12th Mersenne prime $M_{127} = 2^{127} - 1$ (it is the largest prime ever discovered by hand calculations as well as the largest known double Mersenne prime); the first nice Friedman number (the representation $127 = 2^7 - 1$ uses all digits 1, 2, and 7); the smallest prime that can be written as the sum of the first two or more odd primes ($127 = 3 + 5 + 7 + 11 + 13 + 17 + 19 + 23 + 29$).
- **140**: the first even Ore number, which is not perfect; an odious number.
- **144**: the largest, besides 0 and 1, perfect square, which is a Fibonacci number; the sum of a twin prime pair (71; 73).
- **149**: the only known prime in the concatenate square sequence.
- **173**: the largest known prime whose square, 29929, and cube, 5177717, consist of different digits.

- **191**: a palindromic prime whose square 36481 is a distinct-digit number whose first two digits, central digit, and last two digits are perfect squares.
- **196**: the smallest candidate *Lychrel number*, i.e., a natural number which cannot form a palindrome through the iterative process of repeatedly reversing its base 10 digits and adding the resulting numbers; in fact, 196 does not yield a palindrome after 700,000,000 iterations.
- **211**: the largest known prime that cannot be written as a sum of a prime and a positive triangular number.
- **216**: the smallest cubic number, which is a sum of three cubic numbers: $216 = 6^3 = 5^3 + 4^3 + 3^3$.
- **220**: the smallest amicable number; the smaller member of the first amicable pair (220, 284); a practical number; a harshad number.
- **229**: replacing each digit of prime 229 with its square and its cube results in two new primes, 4481 and 88729 respectively, with a palindromic difference of 84248; coincidentally, $229+4481+88729$ is palindromic as well.
- **239**: a Chen prime (241 is a prime); a Sophie Germain prime (479 is a prime); the largest integer, besides 23, which is not a sum of less than 9 cubic numbers: $239 = 2 \cdot 4^3 + 4 \cdot 3^3 + 3 \cdot 1^3$.
- **257**: the fourth Fermat prime, F_3; the largest prime in a sequence of fifteen primes of the form $2n + 17$, where n runs through the first 15 triangular numbers.
- **276**: the smallest number with unknown aliquot sequence; the first of *Lehmer five* 276, 552, 564, 660, and 966; the sum of three consecutive fifth powers ($276 = 1^5+2^5+3^5$); the sum of 12 consecutive prime numbers ($5+7+11+13+17+19+23+29+31+37+41+43$); an untouchable number.
- **277**: the square 76729 of the prime 277 is the smallest square with five or more digits that is a concatenation of three primes ($7, 67$, and 29).
- **284**: the bigger member of the first amicable pair $(220, 284)$.
- **289**: the square of the sum of the first four primes: $289 = (2+3+5+7)^2$.

- **325**: the first 3-hyperperfect number.
- **341**: the first Poulet number, i.e., Fermat pseudoprime to base 2.
- **343**: the only, besides 1, cubic number (7^3) such that the sum of its divisors is a perfect square: $1 + 7 + 7^2 + 7^3 = 20^2$; a *Friedman number*, as it is the result of a non-trivial expression using all its own digits, $343 = (3 + 4)^3$.
- **367**: the largest number (in fact, prime) whose square, 134689, has strictly increasing digits.
- **400**: the only known square of the form $1 + k + k^2 + k^3$, where $k \in \mathbb{N}\backslash\{1\}$ (in fact, $k = 7$).
- **407**: the largest integer, besides $1, 153, 370$, and 371, which is the sum of cubes of their decimal digits.
- **463**: the smallest multi-digit prime such that both the sum of digits and product of digits of its square remain squares.
- **496**: the third perfect number; the smallest triangular number such that the sum of the cubes of its digits is prime: $4^3 + 9^3 + 6^3 = 1009$.
- **541**: the 100th prime number, the 10th hexagonal star (i.e., Star of David) number.
- **561**: the first Carmichael number.
- **576**: the only known perfect square represented as a difference between a squared sum of consecutive primes and the sum of their squares: $576 = 24^2 = (2+3+5+7+11)^2 - (2^2+3^2+5^2+7^2+11^2)$; it is the only such case for all primes up to $2 \cdot 10^9$.
- **631**: a prime which is the reverse concatenation of the first three triangular numbers.
- **641**: the prime divisor of the smallest Fermat composite, F_5: $F_5 = 4294967297 = 641 \cdot 6700417$.
- **691**: the only known prime which is a square, 169, when turned upside down and another square, 196, when reversed; moreover, 169 and 196 are the smallest consecutive squares using the same digits.
- **701**: the smallest prime whose square, 491401, contains all of square digits only; it is equal to $5^4 + 4^3 + 3^2 + 2^1 + 1^0$.
- **727**: the first prime whose square, 528529, can be represented as the concatenation of two consecutive numbers.

- **773**: replacing each digit of the prime 773 with its square respectively its cube results in two new primes, 49499 and 34334327; this latter number is also an *emirp* (72343343 is a prime).
- **786**: the largest known number n such that the binomial coefficient $\binom{2n}{n}$ is not divisible by the square of an odd prime.
- **900**: the smallest perfect square which is a sum of different primes by using all the 10 digits: $900 = 503 + 241 + 89 + 67 = 509 + 283 + 61 + 47$.
- **945**: the first odd semiperfect number.
- **1980**: the smallest member of amicable k-tuples, $k \geq 3$; the smallest amicable triple is (1980, 2016, 2556).
- **2047**: the first Mersenne composite with prime index, M_{11}.
- **4375**: the smallest perfect totient number not divisible by 3.
- **5040**: the largest known number that violates *Robin's inequality*; a superabundant (in fact, a colossally abundant) number.
- **6160**: the smallest augmented amicable number; the smallest pair of augmented amicable numbers is (6160, 11697).
- **8218**: the fourth perfect number.
- **12285**: the smallest odd amicable number; belongs to the amicable pair (12285, 14595).
- **12496**: the smallest sociable number; a member of the first sociable 5-cycle (12496, 14288, 15472, 14536, 14264).
- **20161**: the biggest number which cannot be represented as a sum of two abundant numbers.
- **30240**: the first 4-perfect number.
- **65537**: the biggest known Fermat prime, F_4.
- **1264460**: the smallest member of sociable quadruples; (1264460, 1547860, 1727636 1305184) is the first sociable quadruple.
- **33550336**: the fifth perfect number.
- **4294967297**: the smallest Fermat composite (in fact, semiprime), F_5.
- **5391411025**: the smallest abundant number coprime with 2 and 3.
- **8589869056**: the sixth perfect number.
- $\mathbf{10^{100}}$: one *googol*; in decimal notation, it is written as the digit 1 followed by one hundred zeros; a googol is approximately 70!; 1 googol $\approx 2^{332.19280949}$.

- $\mathbf{2^{2^9}+1=2^{512}+1}$: the first Fermat number, F_9, greater than googol, i.e., having more than 100 digits (in fact, 154 digits).
- **686479...057151**: the first Mersenne prime, $M_{521}=2^{521}-1$, greater than googol, i.e., having more than 100 digits (in fact, 157 digits); the 13th Mersenne prime.
- **235627...646976**: the first perfect number $2^{520}(2^{521}-1)$, greater than googol, i.e., having more 100 digits (in fact, 314 digits); the 13th perfect number.
- $\mathbf{2317006\ldots230657\ =2^{2^{11}}+1=2^{2048}+1}$: the biggest completely factored Fermat number, F_{11}; it has 617 digits; it is a product of five prime numbers with 6, 6, 21, 22, and 564 decimal digits.
- $\mathbf{1000\ldots0007=10^{999}+7}$: the smallest *titanic prime*, i.e., a prime of at least 1,000 decimal digits.
- **190797...484991**: the smallest Mersenne titanic prime, $M_{4253}=2^{4253}-1$; the 19th Mersenne prime; it has 1281 digits.
- **108925...782528**: the smallest titanic perfect number, $2^{2202}(2^{2203}-1)$; the 16th perfect number; it has 1327 digits.
- $\mathbf{2^{2^{33}}+1}$: the smallest Fermat number, F_{33}, with unknown character.
- $\mathbf{1000\ldots00033603=10^{9999}+33603}$: the smallest *gigantic prime*, i.e., a prime number with at least 10000 decimal digits; it has exactly 10000 digits.
- **931144...942656**: the smallest gigantic perfect number, $2^{19936}(2^{19937}-1)$; the 24th perfect number; it has 12003 digits.
- **854509...228671**: the smallest Mersenne gigantic prime, $M_{44497}=2^{44497}-1$; the 27th Mersenne prime; it has 13395 digits.
- $\mathbf{191273\cdot 2^{3321908}-1}$: the smallest known *megaprime*, i.e., a prime with at least one million decimal digits; it has exactly 1000000 digits.
- **437075...193791**: the smallest Mersenne megaprime, $M_{6972593}=2^{6972593}-1$; the 38th Mersenne prime; it has 2098960 digits.
- **194276...462976**: the smallest megaperfect number, $2^{2976220}(2^{2976221}-1)$; the 36th perfect number; it has 1791864 digits.

- **148894...902591**: the biggest known Mersenne prime, $M_{82589933} = 2^{82589933} - 1$; the 51st known Mersenne prime; it has 24862048 digits.
- **110847...207936**: the biggest known perfect number $2^{82589932}(2^{82589933} - 1)$; the 51st known perfect number; it has 49724095 digits.
- $\mathbf{10^{10^{100}} = 10^{\boldsymbol{googol}}}$: one *googolplex*; written out in ordinary decimal notation, it is 1 followed by 10^{100} zeros, that is, a unity followed by a googol zeros.
- $\mathbf{2^{2^{334}} + 1}$: the first Fermat number, F_{334}, greater than googoplex.
- $\mathbf{2^{2^{18233954}} + 1}$: the largest known composite Fermat number, $F_{18233954}$; it has the prime factor $p = 7 \cdot 2^{18233956} + 1$.

This page intentionally left blank

Chapter 7

Mini Dictionary

In this chapter, a mini dictionary, i.e., a list of all special numbers, relative to perfect and amicable numbers, is provided (see [CoGu96], [DeDe12], [Deza17], [Deza18], [Deza21], [Weis22], [Wiki22], etc.).

- $n \in \mathbb{N}$, $\sigma(n) > 2n$ — *abundant numbers* (or *excessive numbers*): positive integers for which their sum of proper divisors is greater than the number itself; *primitive abundant numbers* — abundant numbers which are not the multiples of abundant numbers or perfect numbers.
- $n \in \mathbb{N}$, $\sigma(n) = 2n - 1$ — *almost perfect numbers* (or *slightly defective numbers* or *least deficient numbers*): positive integers for which their sums of proper divisors are equal to $n - 1$.
- $n \in \mathbb{N}$, $\sigma^2(n) = \sigma(\sigma(n)) = 2n - 1$ — *almost superperfect numbers.*
- $n \in \mathbb{N}$, $\sigma^k(n) = \sigma(\dots\sigma(n)) = 2n - 1$, $k \in \mathbb{N}$ — *almost k-superperfect numbers.*
- (m, n), $m, n \in \mathbb{N}$, $\sigma(n) = \sigma(m) = n + m$ — *amicable numbers* (or *amicable pairs*): pairs of positive integers which are the sums of each other's proper divisors.
- (m, n), $m, n \in \mathbb{N}$, $\sigma(m) = \alpha n + m$, $\sigma(n) = \beta m + n$, $\alpha, \beta \in \mathbb{N}$, $\alpha\beta > 1$ — *(α, β)-amicable pairs* (or *multiple amicable pairs* or *multi-amicable pairs*).
- $n \in \mathbb{N}$, $\tau(m) < \tau(n)$ for any $m < n$, $m \in \mathbb{N}$ — *anti-prime numbers* (or *highly composite numbers*); positive integers with more divisors than any smaller positive integer has.

- $(m_1, \ldots, m_k)$, $m_1, \ldots, m_k \in \mathbb{N}$, $\sigma(m_1) = \cdots = \sigma(m_k) = m_1 + \cdots + m_k$ — *amicable multisets.*
- $(m_1, \ldots, m_k)$, $m_1, \ldots, m_k \in \mathbb{N}$, $\sigma(m_1) = \cdots = \sigma(m_k) = m_1 + \cdots + m_k$, $m_1 < \cdots < m_k$ — *amicable k-tuples*; in particular, (m_1, m_2, m_3), $m_1, m_2, m_3 \in \mathbb{N}$, $\sigma(m_1) = \sigma(m_2) = \sigma(m_3) = m_1 + m_2 + m_3$, $m_1 < m_2 < m_3$ — *amicable triples.*
- (m, n), $m, n \in \mathbb{N}$, $\sigma(n) = \sigma(m) = n + m + 1$ — *betrothed numbers* (or *quasi-amicable numbers* or *reduced amicable numbers*); two positive integers such that the sum of the proper divisors of either number is one more than the value of the other number.
- $BC(n) = n^4$, $n = 1, 2, 3, \ldots$ — *biquadratic numbers.*
- $\binom{n}{m}$, $n = 0, 1, 2, \ldots$, $m = 0, 1, \ldots, n$ — *binomial coefficients*; they form the *Pascal's triangle* — number triangle, the sides of which are formed by 1, and any inner entry is obtained by adding the two entries diagonally above.
- $n \in \mathbb{N}, \sigma^{**}(n) = kn, k \in \mathbb{N}$ – *bi-unitary multiply k-perfect numbers* (or *bi-unitary multiperfect numbers*); positive integers which divide the sum of their proper *bi-unitary divisors.*
- $n \in \mathbb{N}, \sigma^{**}(n) = 2n, k \in \mathbb{N}$ – *bi-unitary perfect numbers*; positive integers which are equal to the sum of their proper *bi-unitary divisors.*
- $n \in S$, $a^{n-1} \equiv 1 (mod\, n)$ for any $a \in \mathbb{Z}$, a coprime to n — *Carmichael numbers*: numbers n that are Fermat pseudoprimes to any base a coprime to n.
- $Ca(n) = 4^n - 2^{n+1} - 1$, $n = 1, 2, 3, \ldots$ — *Carol numbers.*
- $CS_m(n) = \frac{mn^2 - mn + 2}{2}$, $n = 1, 2, 3, \ldots$ — *centered m-gonal numbers.*
- $p \in P$ such that $p + 2 \in P$ or $p + 2 = q_1 \cdot q_2$, $q_1, q_2 \in P$ — *Chen primes*: prime numbers p such that $p + 2$ are either primes or semiprimes (a product of two primes).
- $n \in \mathbb{N}$, for which there is an $\epsilon > 0$ such that, for all $k > 1$, $\frac{\sigma(n)}{n^{1+\epsilon}} \geq \frac{\sigma(k)}{k^{1+\epsilon}}$ – *colossally abundant numbers.*
- $n = 2^r \cdot p_1 \cdot \ldots \cdot p_k$, where $r \in \mathbb{Z}$, $r \geq 0$, and $p_1 < \cdots < p_k$ are distinct Fermat primes — *constructible numbers*: line segment of length n can be constructed with compass and straightedge in a finite number of steps.

- $n \in \mathbb{N}$, for which there is $m \in \mathbb{N}$ such that $m - \phi(m) = n$ — *cototient numbers*; positive integers that can be expressed as the difference between a positive integer m and the number of coprime integers below it.
- $C(n) = n^3$, $n = 1, 2, 3, \ldots$ — *cubic numbers* (or *cube numbers*).
- $Cu(n) = n \cdot 2^n + 1$, $n = 1, 2, 3, \ldots$ — *Cullen numbers.*
- $n \in \mathbb{N}$, $\sigma(n) < 2n$ — *deficient numbers*: positive integers, for which their sum of proper divisors is less than the number itself.
- $M_{M_n} = 2^{2^n-1} - 1$, $n = 1, 2, 3, \ldots$ — *double Mersenne numbers.*
- $(1 + \omega)^n - 1$, where $\omega = \frac{-1+i\sqrt{3}}{2}$, $i^2 = -1$, $n = 1, 2, 3, \ldots$ — *Eisenstein Mersenne numbers.*
- 13, 17, 31, 37, 71,… — *emirps*: prime numbers that result in different primes when its decimal digits are reversed.
- $n \in \mathbb{N}$, for which there is $m < n$ such that $n = \sum_{d|n,\ d \leq m} d$ — *Erdős–Nicolas numbers*; positive integers which are equal to one of the partial sums of its divisors.
- 3, 5, 6, 9, 10, 12, 15, 17, 18, 20, … — *evil numbers*; positive integers with an even number of unities in their binary expansion.
- $F_n = 2^{2^n} + 1$, $n = 0, 1, 2, \ldots$ — *Fermat numbers.*
- $n \in S$, n is odd, $a^{n-1} \equiv 1 (mod\ n)$ — *Fermat pseudoprimes* to base a.
- $u_{n+2} = u_{n+1} + u_n$, $u_1 = u_2 = 1$ — *Fibonacci numbers.*
- $n \in \mathbb{N}$, for which there is $m \in \mathbb{N}$, $m \neq n$, such that $\frac{\sigma(m)}{m} = \frac{\sigma(n)}{n}$ — *friendly numbers*; two or more positive integers with a common *abundancy*; two numbers with the same abundancy form a *friendly pair*; k numbers with the same abundancy form a *friendly k-tuple* (or *friendly club*).
- 25, 121, 125, 126, 127,… — *Friedman numbers*: positive integers, represented as the result of a non-trivial expression using all its own digits (e.g., $25 = 5^2$, $121 = 11^2$, $343 = (3 + 4)^3$, etc.).
- $(1 + i)^n - 1$, where $i^2 = -1$, $n = 1, 2, 3, \ldots$ — *Gaussian Mersenne numbers.*
- $n \in \mathbb{N}$ such that $\frac{\sigma_k(m)}{m^k} < \frac{\sigma_k(n)}{n^k}$ for all $m < n$ — *generalized k-super abundant numbers*; 1-superabundant numbers are *superabundant numbers*; 0-super abundant numbers are *highly composite numbers.*

- $p \in P$, $p > 10^{9999}$ — *gigantic primes*: prime numbers with at least 10000 decimal digits.
- $n \in \mathbb{N}$, $n = p+q$, $p, q \in P\backslash\{2\}$ — *Goldbach numbers*: even positive integers that can be expressed as the sum of two odd primes.
- $n \in \mathbb{N}$, $n = \sum_{d|n, d<n, d\in\mathcal{S}} d$, where $\mathcal{S}$ is defined as follows: $1 \in \mathcal{S}$, and for any $n > 1$, $n \in \mathcal{S}$, if $\sum_{d|n, d<n, d\in\mathcal{S}} d \leq n$ — *Granville numbers* (or *$\mathcal{S}$-perfect numbers*); *$\mathcal{S}$-deficient numbers* — numbers n with $\sum_{d|n, d<n, d\in\mathcal{S}} d < n$; *$\mathcal{S}$-abundant numbers* — numbers n with $\sum_{d|n, d<n, d\in\mathcal{S}} d > n$.
- $n \in \mathbb{N}$, $\frac{\tau(n)}{\sum_{d|n} \frac{1}{d}} \in \mathbb{N}$ — *Harmonic divisor numbers* (or *Ore numbers* or *Ore harmonic numbers*); positive integers whose divisors have a *harmonic mean* that is an integer.
- $n \in \mathbb{N}$, $n = (c_s c_{s-1} \dots c_1 c_0)_g$, $g \in \mathbb{N}\backslash\{1\}$, $(\sum_{i=0}^{s} c_i)|n$ — *harshad numbers* (or *Niven numbers* or *g-harshad numbers* or *g-Niven numbers*) *in base g*; integers that are divisible by the sum of its digits when written in that base.
- $n \in \mathbb{N}$, $\sigma(n) = \frac{k}{2} \cdot n$, where k is odd — *k-hemiperfect numbers* (or just *hemiperfect numbers*); positive integers with a half-integral *abundancy.*
- $n \in \mathbb{N}$, $\sigma(m) < \sigma(n)$ for any $m < n$, $m \in \mathbb{N}$ — *highly abundant numbers*; positive integers, for which the sum of their divisors (including itself) is greater than the sum of the divisors of any smaller positive integer.
- $n \in \mathbb{N}$, $\tau(m) < \tau(n)$ for any $m < n$, $m \in \mathbb{N}$ — *highly composite numbers* (or *anti-prime numbers*); positive integers with more divisors than any smaller positive integer has.
- 2, 4, 8, 23, 35, 47, ... — *highly cototient numbers*; positive integers $n > 1$ which have more solutions to the equation $x - \phi(x) = n$ than any integer k, $1 < k < n$.
- $n \in \mathbb{N}$, $n = 1 + k(\sigma(n) - n - 1)$ — *k-hyperperfect numbers*, $k \in \mathbb{N}$; *hyperperfect numbers* — positive integers which are k-hyperperfect numbers for some positive integer k.
- $C^k(n) = n^k$, $n = 1, 2, 3, \dots$ — *k-dimensional hypercube numbers*, $k \in \mathbb{N}$, $k > 1$.
- $Ky(n) = 4^n + 2^{n+1} - 1$, $n = 1, 2, 3, \dots$ — *Kynéa numbers.*

- $L_{n+2} = L_{n+1} + L_n$, $L_0 = 2$, $L_1 = 1$ — *Lucas numbers.*
- $p \in P$, $p > 10^{999999}$ — *megaprimes*: prime numbers with at least one million decimal digits.
- $M_n = 2^n - 1$, $n = 1, 2, 3, \ldots$ — *Mersenne numbers.*
- $S_m(n) = \frac{n((m-2)n-m+4)}{2}$, $n = 1, 2, 3, \ldots$ — *m-gonal numbers.*
- $S_m^3(n) = \frac{n(n+1)((m-2)n-m+5)}{6}$ $n = 1, 2, 3, \ldots$ — *m-gonal pyramidal numbers.*
- (m, n), $m, n \in \mathbb{N}$, $\sigma(m) - m = \alpha n$, $\sigma(n) - n = \beta m$, $\alpha, \beta \in \mathbb{N}$, $\alpha\beta > 1$ — *(α, β)-multiple amicable pairs* (or *(α, β)-multiply amicable pairs* or *multiamicable pairs*).
- $n \in \mathbb{N}$, $\sigma(n) = kn$, $k \in \mathbb{N}$ — *k-perfect numbers* (or *k-fold perfect numbers*); *multiply perfect numbers* — numbers that are k-perfect for some k, i.e., numbers n with $n|\sigma(n)$.
- $n \in \mathbb{N}$, $\sigma^m(n) = \sigma(\ldots\sigma(n)) = kn$, $k, m \in \mathbb{N}$ — *(m, k)-perfect numbers*; perfect numbers are (1, 2)-perfect.
- $n \in \mathbb{N}$, for which there is no $m \in \mathbb{N}$, $m - \phi(m) = n$ — *noncototient numbers*; positive integers that cannot be expressed as the difference between a positive integer m and the number of coprime integers below it.
- $n \in \mathbb{N}$, for which there is no $m \in \mathbb{N}$, $\phi(m) = n$ — *non-totient numbers*; positive integers which are not within the range of the Euler's totient function.
- 1, 2, 4, 7, 8, 11, 13, 14, 16, 19,… — *odious numbers*; positive integers with an odd number of unities in their binary expansion.
- 1, 6, 28, 140, 270, 496,… — *Ore numbers* (or *harmonic divisor numbers*): positive integers whose divisors have a harmonic mean that is an integer (e.g., the harmonic mean $\frac{4}{\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{6}}$ of divisors 1, 2, 3, and 6 of 6 is an integer 2).
- $(abc \ldots cba)_{10}$ — *palindromic numbers* (or *numeral palindromes* or *numeric palindromes*): positive integers that remain the same when their decimal digits (in general, digits in any positional number system) are reversed (e.g., 16461).
- 2, 3, 5, 7, 11, 13, … — *permutable primes* (or *absolute primes*): prime numbers which remain primes on every rearrangement of their decimal digits; in general, digits in any positional number

system (e.g., 337 is a permutable prime because each of 337, 373, and 733 is prime).

- $n \in \mathbb{N}$, $\sigma(n) = 2n$ — *perfect numbers*; positive integers equal to the sum of their proper divisors.
- 3, 9, 15, 27, 39, 81, 111,… — *perfect totient numbers*; positive integers equal to the sums of their iterated totients.
- 3, 5, 6, 7, 9,… — *pernicious numbers*: positive integers such that the *Hamming weights* of their binary representations (i.e., the sums of binary digits) are primes (e.g., $3 = 11_2$ and $1 + 1 = 2$, $2 \in P$).
- $2^u 3^v + 1 \in P$, where $u, v \in \mathbb{Z}$, $u, v \geq 0$ — *Pierpont primes.*
- $2^u 3^v - 1 \in P$, where $u, v \in \mathbb{Z}$, $u, v \geq 0$ — *Pierpont primes of the second kind.*
- $n \in S$, n is odd, $2^{n-1} \equiv 1 (mod\ n)$ — *Poulet numbers* (or *Sarrus numbers*): Fermat pseudoprimes to base 2.
- 1, 3, 5, 6, 7, 9, 10, 11, 12, 13, … — *polite numbers*: positive integers that can be represented as the sum of two or more consecutive positive integers.
- 1, 2, 4, 6, 8, 12, … — *practical numbers* (or *panarithmic numbers*): positive integers n such that all smaller positive integers can be represented as sums of distinct divisors of n.
- $n\sharp$ — *primorial* of a positive integer n: the product of all primes less than or equal to n.
- $P(n) = n(n + 1)$, $n = 1, 2, 3, \ldots$ — *pronic numbers.*
- $k \cdot 2^n + 1$, $k \in \mathbb{N}$, k is odd, $k < 2^n$ — *Proth numbers.*
- (m, n), $m, n \in \mathbb{N}$, $\sigma(n) = \sigma(m) = n + m + 1$ — *quasi-amicable numbers* (or *betrothed numbers* or *reduced amicable numbers*).
- $n \in \mathbb{N}$, $\sigma(n) = 2n+1$ — *quasi-perfect numbers* (or *slightly abundant numbers*); abundant numbers with *abundance* 1.
- $(x_1, x_2, \ldots, x_k)$, $x_i \in \mathbb{N}$, $s(x_1) - 1 = x_2$, $s(x_2) - 1 = x_3, \ldots$, $s(x_{k-1}) - 1 = x_k$, $s(x_k) - 1 = x_1$ — *quasi-sociable numbers* (or *quasi-sociable sequences* or *quasi-sociable chains* or *quasi-sociable k-tuples*); positive integers whose aliquot sums minus one form a cyclic sequence that begins and ends with the same number.
- $n \in \mathbb{N}$, $\sigma^2(n) = \sigma(\sigma(n)) = 2n + 1$ — *quasi-superperfect numbers.*
- $n \in \mathbb{N}$, $\sigma^k(n) = \sigma(\ldots\sigma(n)) = 2n + 1$ — *quasi k-superperfect numbers.*

- $n \in \mathbb{N}$, $n = \frac{u(u+1)}{2} = 2^v - 1$, $u \geq 0$, $v \geq 0$ — *Ramanujan–Nagell numbers*: the numbers 0, 1, 3, 15, 4095, which are the only non-negative integers which have simultaneously the form $\frac{u(u+1)}{2}$, $u = 0, 1, 2, \dots$ and the form $2^v - 1$, $v = 0, 1, 2, \dots$.
- $n \in \mathbb{N}$, $\tau(n)|n$ — *refactorable numbers* (or *tau numbers*): positive integers that are divisible by the number of their divisors.
- $(aaa \dots aaa)_{10}$ — *repdigits* (or *monodigits*): positive integers composed of repeated instances of the same digit in decimal system (in general, in any positional number system).
- $(111 \dots 111)_{10}$ — *repunits*: positive integers containing only the digit 1 in decimal system (in general, in any positional number system); $R_n = \frac{10^n - 1}{9}$.
- 509203, 762701, 777149, 790841, 992077, … — *Riesel numbers*: odd positive integers k such that $k \cdot 2^n - 1$ is composite for all natural numbers n.
- $n \in \mathbb{N}$, $n = \sum_{d|n, d<n, d \in \mathcal{S}} d$, where $\mathcal{S}$ is defined as follows: $1 \in \mathcal{S}$, and for any $n > 1$, $n \in \mathcal{S}$ if $\sum_{d|n, d<n, d \in \mathcal{S}} d \leq n$ — *$\mathcal{S}$-perfect numbers* (or *Granville numbers*).
- $q = 2p + 1 \in P$, where $p \in P$ — *safe primes*; q is the prime number $2p + 1$ associated with a *Sophie Germain prime* p.
- 6, 12, 18, 20, 24, 28, … — *semiperfect numbers* (or *pseudoperfect numbers*): positive integers that are equal to the sum of all or some of their proper divisors; *primitive semiperfect numbers* (or *primitive pseudoperfect numbers* or *irreducible semiperfect numbers* or *irreducible pseudoperfect numbers*) — semiperfect numbers that have no semiperfect proper divisors.
- $p \cdot q$, $p, q \in P$ — *semiprimes*: positive integers, which are product of two primes.
- 78557, 271129, 271577, 322523, 327739,… — *Sierpiński numbers*: odd positive integers k such that $k \cdot 2^n + 1$ are composite for all natural numbers n.
- $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$, $p_1 < \cdots < p_s \leq k$ — *k-smooth numbers* (or *k-friable numbers*); positive integers whose prime factors are all less than or equal to k.

- $(m_1, \dots, m_k)$, $m_i \in \mathbb{N}$, $m_1 < m_2 < \cdots < m_k$, $s(m_1) = m_2$, $s(m_2) = m_3, \dots,$ $s(m_{k-1}) = m_k$, $s(m_k) = x_1$ — *sociable numbers* (or *sociable k-tuples* or *aliquot k-cycles* or *sociable groups of order k*).
- $n \in \mathbb{N}$, for which there is no $m \neq n$ with $\frac{\sigma(m)}{m} = \frac{\sigma(n)}{n}$ — *solitary numbers*: positive integers which have no friends.
- $p \in P$ such that $2p + 1 \in P$ — *Sophie Germain primes*: the prime number $q = 2p + 1$ associated with p is called *safe prime*.
- 1, 2, 3, 5, 6, 7, 10, 11, 13, 14, ... — *square-free numbers* (or *square-free integers*): integers which are divisible by no perfect squares other than 1 (that is, their prime factorizations have exactly one factor for each prime that appears in it).
- 0, 1, 8, 11, 69, 88, 96, 101, ... — *strobogrammatic numbers*: positive integers whose numeral is rotationally symmetric so that it appears the same when rotated 180 degrees.
- $n \in \mathbb{N}$, for which $\tau(n)$ and $\sigma(n)$ are both perfect — *sublime numbers*.
- $n \in \mathbb{N}$, $\frac{\sigma(m)}{m} < \frac{\sigma(n)}{n}$ for any $m < n$, $m \in \mathbb{N}$ — *superabundant numbers*: abundant numbers whose relative abundance is greater than for any smaller number.
- $n \in \mathbb{N}$, for which there is an $\epsilon > 0$ such that, for all $k > 1$, $\frac{\tau(n)}{n^\epsilon} \geq \frac{\tau(k)}{k^\epsilon}$ — *superior highly composite numbers*: positive integers which have more divisors per some positive power of itself than any other number.
- $n \in \mathbb{N}$, $\sigma^2(n) = \sigma(\sigma(n)) = 2n$ — *superperfect numbers*.
- $n \in \mathbb{N}$, $\sigma^k(n) = \sigma(\dots\sigma(n)) = 2n$ — *k-superperfect numbers*.
- $3 \cdot 2^n - 1$, $n \in \mathbb{Z}, n \geq 0$ — *Thābit numbers* (or *Thābit ibn Qurra numbers* or *321 numbers*); *Thābit primes*: prime numbers of this form.
- $3 \cdot 2^n + 1$, $n \in \mathbb{Z}, n \geq 0$ — *Thābit numbers of the second kind*; *Thābit primes of the second kind*: prime numbers of this form.
- For a given $b \geq 2$, $(b+1) \cdot b^n - 1$, $n \in \mathbb{Z}, n \geq 0$ — *Thābit numbers base b*; *Thābit primes base b*: prime numbers of this form.
- For a given $b \geq 2$, $(b+1) \cdot b^n + 1$, $n \in \mathbb{Z}, n \geq 0$ — *Thābit numbers of the second kind base b*; *Thābit primes of the second kind base b*: prime numbers of this form.

- $p \in P, p > 10^{999}$ — *titanic primes*: prime numbers of at least 1000 decimal digits.
- $Tr(n,k) = n + (n+1) + \cdots + (n + (k-1)),\ n, k \in \mathbb{N}\backslash\{1\}$ — *trapecoidal numbers*.
- $S_3(n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2},\ n \in \mathbb{N}$ — *triangular numbers*.
- $n \in \mathbb{N}$, for which there is $m \in \mathbb{N}$, $\phi(m) = n$ — *totient numbers*: values of the Euler's totient function.
- $n \in \mathbb{N}$, $\sigma^*(n) = 2n$, $k \in \mathbb{N}$ — *unitary perfect numbers*: positive integers which are equal to the sum of their proper *unitary divisors*.
- 2, 5, 52, 88, 96, 120, 124, 146, 162, 188, ... — *untouchable numbers*: positive integers that cannot be expressed as the sum of all the proper divisors of any positive integer (including the untouchable number itself).
- $\frac{2^p+1}{3} \in P$, where $p \in P$ — *Wagstaff primes*.
- 70, 836, 4030, 5830, 7192, ... — *weird numbers*: abundant numbers which are not semiperfect; *primitive weird numbers*: weird numbers which have no proper weird divisors.
- For a given $b \geq 2$, $(b-1) \cdot b^n - 1$, $n \in \mathbb{Z}, n \geq 0$ — *Williams numbers base b*; *Williams primes base b*: prime numbers of this form.
- For a given $b \geq 2$, $(b-1) \cdot b^n + 1$, $n \in \mathbb{Z}, n \geq 0$ — *Williams numbers of the second kind base b*; *Williams primes of the second kind base b*: prime numbers of this form.
- $W_n = n \cdot 2^n - 1,\ n = 1, 2, 3, \ldots$ — *Woodall numbers* (or *Cullen numbers of the second kind*).

This page intentionally left blank

Chapter 8

Exercises

Problems, Connected with Arithmetic Functions

1. Prove that $f(n) = gcd(n, k)$ (the greatest common divisor of n and k), where k is a fixed integer, is a multiplicative function; is it completely multiplicative?
2. Prove that $f(n) = (\frac{n}{p})$ (the *Legendre symbol*), where p is a fixed odd prime number, is a completely multiplicative function.
3. Prove that any Dirichlet character modulo n is a completely multiplicative function.
4. Prove that the Dirichlet convolution $f * g$ of two multiplicative functions f and g, defined by $(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$, where the sum extends over all positive divisors d of n, is a multiplicative function.
5. Prove that if f is a multiplicative function and a, b are any two positive integers, then $f(a) \cdot f(b) = f(gcd(a, b)) \cdot f(lcm(a, b))$.
6. Prove that $n! = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, where p_i are all primes less than or equal to n, and
$$\alpha_i = \left\lfloor \frac{n}{p_i} \right\rfloor + \left\lfloor \frac{n}{p_i^2} \right\rfloor + \left\lfloor \frac{n}{p_i^3} \right\rfloor + \cdots .$$
7. Prove that the greatest α such that $p^\alpha | \binom{2n}{n}$ is $\sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right)$.

8. Prove that $\sum_{n=1}^{\frac{q}{2}}\lfloor\frac{np}{q}\rfloor+\sum_{m=1}^{\frac{p}{2}}\lfloor\frac{mq}{p}\rfloor=\frac{p-1}{2}\cdot\frac{q-1}{2}$, where $m,n\in\mathbb{N}$, $p,q\in P\backslash\{2\}$, and $p\neq q$.
9. Prove that for any real non-integer number x, there exists the following decomposition:
$$\lfloor x\rfloor=x-\frac{1}{2}+\frac{1}{\pi}\sum_{k=1}^{\infty}\frac{\sin(2\pi kx)}{k}.$$
10. Find $\sum_{k=0}^{\infty}\frac{\phi(p^k)}{p^{ks}}$, where $s\in\mathbb{R}$ and $s>1$.
11. Find $|\{x\in\mathbb{N}:x\leq km,(x,m)=1\}|$, where $k,m\in\mathbb{N}$.
12. Prove that the function $f(x)=\lfloor\cos^2\pi\frac{(x-1)!+1}{x}\rfloor$ gives the value 1 if x is prime and 0 if x is composite; moreover, $f(1)=1$.
13. Prove the infiniteness of primes using Fermat numbers.
14. Prove the infiniteness of primes in the arithmetic progression $4k+1$ using Fermat numbers.
15. Given $t\in\mathbb{N}$, prove the infiniteness of primes in the arithmetic progression 2^tk+1 using Fermat numbers.
16. Given $p\in P$ and $t\in\mathbb{N}$, prove the infiniteness of primes in the arithmetic progression $2p^tk+1$.
17. Prove the infiniteness of primes using Mersenne numbers.
18. Prove that $\pi(x)\geq\log_2\log_2 x+4$ for any $x\geq 17$.
19. Prove that if f is a completely multiplicative function and $\sum_{n=1}^{\infty}f(n)$ is absolutely convergent for $Re\ s>1$, then $\sum_{n=1}^{\infty}f(n)=\prod_p(1-f(p))^{-1}$.
20. Prove that $\frac{1}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}$ for $Re\ s>1$.
21. Prove that $\sum_{n=1}^{\infty}\frac{\tau(n)}{n^s}=\zeta^2(s)$ for $Re\ s>1$.
22. Prove that, for $Re\ s>1$ and $\zeta^k(s)=\sum_{n=1}^{\infty}\frac{\tau_k(n)}{n^s}$, where $\tau_k(n)=\sum_{n=n_1\ldots n_k}1$ is the number of representations of a given positive integer n as a product of k positive integers, $k\geq 2$.
23. Find all solutions of the equation $\tau(n)=\tau(n+1)$ in the interval $[1,100]$.
24. Find several solutions to the equation $\sigma(n)=\sigma(n+1)$.
25. Prove that $\sigma(n)$ is the total number of even parts in the partitions of 2^n into equal parts.
26. Check that $\sigma(n)$ is the sum of number of common divisors of n and m, where m runs from 1 to n.

27. Check that $\sigma(n)$ is a power of 2 if and only if $n = 1$ or n is a product of distinct Mersenne primes.
28. Find a solution to the equation $\sigma(q^{p-1}) = r^s$ with primes p, q, r, and s.
29. Let $n = pq$ be a product of two distinct primes. Prove that knowing $\sigma(n)$ and $\phi(n)$ allows us to find p and q.
30. Prove that

$$\begin{aligned}\sigma(n) &= \sigma(n-1) + \sigma(n-2) - \sigma(n-5) - \sigma(n-7)\\ &\quad + \sigma(n-12) + \sigma(n-15) + \cdots\\ &= \sum_{i\in\mathbb{Z}}(-1)^{i+1}\left(\sigma\left(n - \frac{1}{2}\left(3i^2 - i\right)\right)\right.\\ &\quad \left. + \ \sigma\left(n - \frac{1}{2}\left(3i^2 + i\right)\right)\right),\end{aligned}$$

where $\sigma(0) = n$ if it occurs, $\sigma(i) = 0$ for $i \leq 0$, and $\frac{1}{2}\left(3i^2 - i\right)$ are the *pentagonal numbers*.

31. Let $\tau_k(n) = \sum_{n=n_1\cdot\ldots\cdot n_k} 1$ be the number of representations of n as a product of k positive integers. Prove that $\tau_2(n) = \tau(n)$. Prove that

$$\tau_k(p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s}) = \frac{(\alpha_1 + k - 1)!}{(k-1)!\alpha_1!}\cdot\ldots\cdot\frac{(\alpha_s + k - 1)!}{(k-1)!\alpha_s!}.$$

32. Prove that for the *mean value* of the Euler's totient function $\phi(n)$, it holds that

$$\sum_{d=1}^{N}\phi(n) = \frac{3N^2}{\pi^2} + O(N\log N),\ \ N \in \mathbb{N}.$$

33. Find the number of integer points under the parabola $y = -ax^2$.
34. Find the number of integer points in an ellipse.
35. Prove that the number of square-free numbers less than or equal to the positive real number x is $\frac{6}{\pi^2}x + O(\sqrt{x})$.
36. Prove that the number of k-free numbers less than or equal to positive real number x is $\frac{x}{\zeta(k)} + O(\sqrt[k]{x})$.

Problems, Connected with Perfect Numbers

1. How many decimal digits have the perfect number 2^{11212} $(2^{11213}-1)$?
2. Prove that if p is a prime, then the Mersenne number M_p is prime or pseudoprime to base 2.
3. Prove that a Mersenne prime cannot be a Wieferich prime, where a *Wieferich prime* is a prime number p such that p^2 divides $2^{p-1}-1$.
4. Prove that any odd positive integer n divides infinitely many Mersenne numbers.
5. A sequence $p, 2p+1, 2(2p+1)+1, \ldots$, in which all of the numbers are primes, is called a *Cunningham chain of the first kind*. Find several Cunningham chains of the first kind. Prove that every term of such a sequence except the last is a *Sophie Germain prime* and every term except the first is a *safe prime*.
6. A sequence $p, 2p-1, 2(2p-1)-1, \ldots$, in which all of the numbers are primes, is called a *Cunningham chain of the second kind*. Find several Cunningham chains of the second kind.
7. Check that any positive integer greater than 20161 is a sum of two abundant numbers.
8. Find all even numbers less than 1000 of the form x^3+1. Check that the only perfect number of such form is 28.
9. A *k-smooth* (or *k-friable*) number is an integer whose prime factors are all less than or equal to k. Find the first five k-smooth numbers for each $k \leq 7$.
10. A positive integer n is a *sublime number* if $\tau(n)$ and $\sigma(n)$ are both perfect. Check that 12 is a sublime number.
11. A *highly cototient number* is a positive integer $n > 1$ which has more solutions to the equation $x - \phi(x) = n$ than any other integer $1 < k < n$. Find the first five highly cototient numbers.
12. A *highly totient number* n is an integer that has more solutions to the equation $\phi(x) = n$ than any integer below it. Find the first five highly totient numbers. Show that the sequence of highly totient numbers is a subset of the sequence of the smallest numbers n with exactly m solutions to the equation $\phi(x) = n$.

13. Find all two-digit *refactorable numbers* n (i.e., such that $\tau(n)|n$). Check that there are no three consecutive refactorable numbers.
14. Find several solutions to the equation $gcd(n, x) = \tau(n)$ for $n = 1, 2, 3, \ldots, 10$. Check that this equation has solutions only if n is a refactorable number, i.e., if $\tau(n)|n$.
15. A *multiplicative perfect number* is a positive integer n such that the product of all its proper divisors is equal to n. Find the first five such numbers.
16. A divisor d of n is called a *unitary divisor* of n if d is relatively prime to $\frac{n}{d}$. Find all unitary divisors of $n = 1, 2, 3, \ldots, 15$. Find the number $\tau^*(n)$ and sum $\sigma^*(n)$ of all unitary divisors of n for $n = 1, 2, 3, \ldots, 15$.
17. A positive integer divisor d of a positive integer n is called a *bi-unitary divisor* of n if the greatest common unitary divisor of d and $\frac{n}{d}$ us equal to 1. Using the sum $\sigma^{**}(n)$ of the bi-unitary divisors of n, check that 120 is a bi-unitary 3-perfect number and that 2 and 9 are bi-unitary superperfect numbers.
18. A divisor d of n is called a *k-ary divisor* of n if the greatest common $(k-1)$-ary divisor of d and $\frac{n}{d}$ is 1. A divisor p^β of p^α, $\alpha \in \mathbb{N}$, is called an *infinitary divisor* of p^α if p^β is an $(\alpha-1)$-ary divisor of p^α. Find all infinitary divisors of $n = 1, 2, 3, \ldots, 15$. Find the number and sum of all infinitary divisors of n for $n = 1, 2, 3, \ldots, 15$.
19. Let $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}$ be an *exponential divisor* of $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ if each $\beta_i|\alpha_i$, $i = 1, 2, \ldots, s$. Find all exponential divisors of $n = 1, 2, 3, \ldots, 15$. Define an *exponential perfect number*. Prove that there are infinitely many exponential perfect numbers.
20. Check that if k is an integer and $2^n - (2k+1)$ is a prime, then $2^{n-1}(2^n - (2k+1))$ is a solution of the equation $\sigma(x) = 2(x+k)$.
21. An *Erdős–Nicolas number* is a number that is not perfect but that equals one of the partial sums of its divisors: there exists $m < n$ such that $\sum_{d|n,\ d\leq m} d = n$. Check that the first Erdős–Nicolas number is 24.
22. Check that any known almost perfect number gives the number of subsets of an finite set as well as the compositions (ordered partitions) of some positive integer.

23. Prove that if $a(n)$ is a 4-perfect number, $k > 1$, and $p = \frac{a(n)}{2^{k-2}} + 1$ is a prime, then, for each positive integer m, $2^{k-1} \cdot p^m$ is a solution to the equation $\sigma(\phi(x)) = 2 \cdot x - 2^k$.
24. A *hemiperfect number* is a positive integer with a half-integral *abundancy index*. For a given odd number k, a number n is called k*-hemiperfect* if and only if the sum of all positive divisors of n is equal to $\frac{k}{2} \cdot n$. Check that 2 is the first 3-hemiperfect number, 24 is the first 5-hemiperfect number, 4 is the first 7-hemiperfect number, 8 is the first 9-hemiperfect number, and 17 is the first 11-hemiperfect number.
25. Check that the first 10 *superabundant numbers* are *harshad numbers*.
26. Find several *perfect totient numbers* of the form $3p$, $p \in P$. Check that in this case, $p \equiv 1(mod\ 4)$.
27. Check that $M_7 = 127$ is a *palindromic prime* in nonary and binary. Are there palindromic Thābit numbers?

Problems, Connected with Amicable Numbers

1. Consider a proposition: *If all three numbers*

$$2^{n+1} - 1 + 2^n,\ 2^{n+1} - 1 - 2^{n-1},\ 2^{n+1}(2^{n+1} + 2^{n-2}) - 1$$

are primes, then the numbers

$$2^n(2^{n+1} - 1 + 2^n)(2^{n+1} - 1 - 2^{n-1}),\ 2^n(2^{n+1}(2^{n+1} + 2^{n-2}) - 1)$$

are amicable. Check that this is the *Thābit's rule.*
2. Prove that if $m \equiv 0(mod\ 6)$ and $n = \sigma(m) - m$ is even, then the pair (m, n) cannot be amicable.
3. Check that the following method can be used for generating amicable pairs of the form $(M, N) = (a_1pq, a_2s)$, $a_1 \neq a_2$ (see [Yan96]): *Let* a_1, a_2 *be two given positive integers; define*

$$A = \sigma(a_1)(\sigma(a_2) - a_2),\ B = a_1\sigma(a_2) - \sigma(a_1)(\sigma(a_2) - a_2)$$

and write $R = \sigma(a_2)(a_1a_2\sigma(a_2) + \sigma(a_1)(a_1 - a_2)(\sigma(a_2) - a_2))$ *as a product* uv*; if*

$$p = \frac{u + A}{B},\ q = \frac{v + A}{B},\ s = \frac{\sigma(a_1)(pq + p + q + 1)}{\sigma(a_2)} - 1$$

are different primes and $gcd(a_1, p) = (a_1, q) = (a_2, s) = 1$, *then* $(M, N) = (a_1pq, a_2s)$ *is an amicable pair.*

4. Check that the following general algebraic method can be used for constructing amicable pairs: *For given* a_1, a_2, *let* $A_1 = \sigma(a_1)$ *and* $A_2 = \sigma(a_2)$*; if* $\frac{a_1}{A_1} + \frac{a_2}{A_2} > 1$, *consider all possible decompositions* $XY = A_2(a_1a_2A_2 + A_1(a_1 - a_2)(a_1 - A_2))$*; if*

$$p = \frac{X + A_1(A_2 - a_2)}{a_1A_2 - A_1(A_2 - a_2)},\ q = \frac{Y + A_1(A_2 - a_2)}{a_1A_2 - A_1(A_2 - a_2)},$$

$$r = \frac{A_1(p + 1)(q + 1)}{A_2} - 1$$

are all primes and $gcd(a_1, p) = gcd(a_1, q) = gcd(a_2, r) = 1$, *then* $(M = a_1 \cdot p \cdot q, N = a_2 \cdot r)$ *is an amicable pair.*

5. Check that the following general algebraic method can be used for constructing amicable pairs (Yan, 1996, [Yan96]): *Let* (a_1p, a_2q) *be a given amicable pair with* p, q *primes and* $(a_1, p) = (a_2, q) = 1$; *select* (a_1, a_2) *to find a solution* (q_1, q_2) *of the bilinear Diophantine equation*

$$(Aq_1 - B)(Aq_2 - B) = AC + B^2,$$

$$\textit{where } A_1 = \sigma(a_1),\ A_2 = \sigma(a_2),$$

$$B_1 = \sigma(a_1) - a_1,\ B_2 = \sigma(a_2) - a_2,$$

$$A = a_1a_2 - B_1B_2,\ B = B_1A_2,\ C = a_1A_1 + B_1A_2;$$

by writing $W = AC + B^2$ *in all possible ways as a product* $W = UV$, *let*

$$q_1 = \frac{U + B}{A},\ q_2 = \frac{V + B}{A},\ p = \frac{a_1q_1q_2 - A_1}{B_1};\quad \textit{if}$$

$$q_1, q_2, p_1 \in \mathbb{N},\ q_1, q_2, p_1 \in P,\ q_1 \neq q_2,\ gcd(a_2, q_1q_2) = 1,$$

$$gcd(a_1, p_1) = 1,$$

then $(a_1p_1, a_2q_1q_2)$ *is an amicable pair.*

6. Check that the following *forward method* can be used to construct an amicable pair $(M, N) = (wpq, ws)$, where p, q, s are primes, $w = gcd(M, N)$, and $gcd(w, pq) = gcd(w, s) = 1$: *Let* $w > 1$ *be a given integer and write* w^2 *as a product* $w^2 = uv$ *with* $2 \leq u \leq v$; *let* $A = \sigma(w) - w$, $B = 2w - \sigma(w)$; *if* $p = \frac{u+A}{B}$, $q = \frac{v+A}{B}$, $s = pq + p + q$ *are distinct primes and* $gcd(w, p) = gcd(w, q) = gcd(w, s) = 1$, *then* $(M, N) = (wpq, ws)$ *is an amicable pair.*
7. Prove that the *Euler's rule* can be considered as a special case, $w = 2^n$, of the above *forward method.*
8. Check that the following *backward method*, starting with two given numbers m and n, can be used for generation an amicable pair $(M, N) = (wm, wn)$: *Let* (m, n) *be a pair of positive integers such that* $\sigma(m) = \sigma(n) \neq m + n$, $m < n$; *if there exists another integer* $w > 1$ *such that* $gcd(m, w) = gcd(n, w) = 1$, $\frac{\sigma(w)}{w} = \frac{m+n}{\sigma(m)}$, *then* $(M, N) = (wm, wn)$ *is an amicable pair.*
9. Check that the sequence 1215571544, 1270824975, 1467511664, 1512587175, 1530808335, 1579407344, 1638031815, 1727239544, 1215571544, ... (sequence A309227 in the OEIS) is a quasi-sociable of order 8.
10. Does the sequence 243902764, 270193365, 263191852, 348188373, 145417011280, 220890775665, 183450487696, 232210408305 forms an augmented aliquot cycle?
11. Check the following algebraic rule for aliquot 4-cycles: *If* $a_1, a_2, d_1, d_2 \in \mathbb{N}$, $a_1 a_2 = d_1 d_2$ *and for* $i = 1, 2$,

$$p_i = \frac{s(a_2)\sigma(a_1) + d_i\sigma(a_2)}{a_1 a_2 - s(a_1)s(a_2)}, \; q_i = \frac{s(a_1)\sigma(a_2) + d_i\sigma(a_1)}{a_1 a_2 - s(a_1)s(a_2)},$$

$$r = \frac{s(a_1 p_1 p_2)}{a_1}, \; t = \frac{s(a_2 q_1 q_2)}{a_2}$$

are all integral and primes, $p_1 \neq p_2$, $q_1 \neq q_2$, *and* $gcd(p_1, a_1) = gcd(p_2, a_1) = gcd(r, a_1) = gcd(q_1, a_2) = gcd(q_2, a_2) = gcd(t, a_2) = 1$, *then* $(m_1, m_2, m_3, m_4) = (a_1 p_1 p_2, a_1 r, a_2 q_1 q_2, a_2 t)$ *is an aliquot* 4*-cycle.*

12. Check the following algebraic rule for aliquot 4-cycles (see [Yan96]): *For a given* n, *let* $a_1 = 2 \cdot 5 \cdot 7^n$ *and* $a_2 = 2 \cdot 11 \cdot 7^n$;

if for some $0 \leq \lambda \leq 2n$, *the following six numbers*

$$p_1 = \frac{2}{3}(7^\lambda + 5 \cdot 7^n) - 1,\ p_2 = \frac{10}{3}(11 \cdot 7^{2n-\lambda} + 7^n) - 1,$$

$$q_1 = \frac{1}{3}(7^\lambda + 11 \cdot 7^n) - 1,$$

$$q_2 = \frac{10}{3}(5 \cdot 7^{2n-\lambda} + 7^n) - 1,\ r = \frac{1}{a_1}s(m_1),\ t = \frac{1}{a_2}s(m_3)$$

are all primes, then $(m_1, m_2, m_3, m_4) = (a_1p_1p_2, a_1r, a_2q_1q_2, a_2t)$ *forms an aliquot* 4-*cycle.*

13. An aliquot sequence for a given integer k can be represented as a directed path in the directed graph $G_{n,s}$ on n vertices $\{1, 2, 3, \dots, n\}$ with arcs $\langle i, s(i)\rangle$, where $s(i)$ denotes the sum of the proper divisors of i. Construct the directed graph $G_{n,s}$ for $n = 10$; for $n = 15$. How many components have these digraphs? Are there cycles in these digraphs?
14. Check that the pair $(12146750, 16247745)$ forms a reduced amicable pair.
15. Check that the pairs $(6160, 11697)$, $(12220, 16005)$, $(23500, 28917)$, and $(9026235, 9843526)$ are augmented amicable pairs.

Solutions to Problems, Connected with Arithmetic Functions

1. The greatest common divisor of n and k is a multiplicative function $f(n) = gcd(n, k)$ because

$$f(mn) = gcd(mn, c) = gcd(m, c) \cdot gcd(n, c) = f(n) \cdot f(m)$$

for any coprimes m and n. It is not completely multiplicative: For example,

$$gcd(2 \cdot 8, 20) = 4 \neq 2 \cdot 4 = gcd(2, 20) \cdot gcd(8, 20).$$

2. By properties of the Legendre symbol, it holds that $(\frac{ab}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p})$ for any $a, b \in \mathbb{Z}$.
3. By definition, for all integers a and b, it holds that $\chi(ab) = \chi(a)\chi(b)$. It is easy to check that the Jacobi symbol is an example of Dirichlet character and hence is a completely multiplicative function.

4. For relatively prime integers a, b, it holds that
$$\begin{aligned}(f * g)(ab) &= \sum_{d|ab} f(d)g\left(\frac{ab}{d}\right)\\ &= \sum_{d_1|a}\sum_{d_2|b} f(d_1d_2)g\left(\frac{ab}{d_1d_2}\right)\\ &= \sum_{d_1|a} f(d_1)g\left(\frac{a}{d_1}\right)\cdot\sum_{d_2|b} f(d_2)g\left(\frac{b}{d_2}\right)\\ &= (f*g)(a)\cdot(f*g)(b).\end{aligned}$$
With the Dirichlet convolution, the set of all multiplicative functions turns into an abelian group; the identity element is ϵ.
5. It follows from the fact that $ab = gcd(a, b) \cdot lcm(a, b)$ and $gcd\left(\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)}\right) = 1$.
6. See, for example, [Buch09].
7. It follows from the prime decomposition that $n! = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ of $n!$, as $\binom{2n}{n} = \frac{(2n)!}{n!n!}$.
8. See a proof of the *quadratic reciprocity law* in [Buch09].
9. The fractional part function $\{x\}$ has *Fourier series* expansion $\{x\} = \frac{1}{2} - \frac{1}{\pi}\sum_{k=1}^{\infty}\frac{\sin(2\pi kx)}{k}$ for x not an integer. Now, we can obtain the result using the formula $\lfloor x \rfloor = x - \{x\}$. For more explanation, see [Titc87].
10. Use the formula $\phi(p^k) = p^k(1-\frac{1}{p})$. Note that the *Dirichlet series* for $\phi(n)$ can be written in terms of the Riemann zeta function as $\sum_{n=1}^{\infty}\frac{\phi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$. See, for example, [HaWr79].
11. In fact, $|\{x \in \mathbb{N} : x \leq km, (x, m) = 1\}| = k\phi(m) = km\prod_{p|m}(1 - \frac{1}{p})$.
12. See the *Wilson theorem*: Any number x is a prime if and only if $(x - 1)! + 1$ is divisible by x. See also [Deza21].
13. Let q_n be the least prime divisor of F_n. As $gcd(F_m, F_n) = 1$ for $n \neq m$, then $q_n \neq q_m$, and we obtain infinitely many primes $q_0, \ldots, q_k, \ldots$.
14. Note that any prime divisor of F_n, $n \geq 1$, has the form $4k + 1$, and use the previous consideration.

15. For $t > 2$, consider the numbers $F_t, F_{t+1}, \dots, F_{t+l}, \dots$. Each such number F_{n+l} has a prime divisor of the form $2^{t+l+2}k+1 = 2^t s+1$.
16. See, for example, [Step01], [Deza17], and [DeKo13].
17. Let $q_i | M_{p_i}$; as $gcd(M_{p_i}, M_{p_j}) = 1$, then $q_i \neq q_j$; if the set $P = \{p_1, \dots, p_k\}$ of primes is finite, then $P = \{q_1, \dots, q_k\}$, but $p_1 = 2$, while all q_i are odd; a contradiction.
18. Let $x \in [p_n, p_{n+1}]$. Then, $\pi(x) = \pi(p_n) = n$. Moreover, $x \leq p_{n+1} \leq 2^{2^{n-4}} + 1$, i.e., $x \leq 2^{2^{n-4}}$ or $\log_2 \log_2 x \leq n - 4$. Now, we obtain that $\pi(x) = n \geq \log_2 \log_2 x + 4$.
19. In this case, we can use that $(1 - f(p))^{-1} = 1 + f(p) + f(p^2) + \cdots + f(p^n) + \cdots$.
20. See, for example, [Titc87], [Kara83], and [Ivic85].
21. It follows from the fact that $\tau(n) = \tau_2(n) = \sum_{n_1 \cdot n_2 = n} 1$.
22. It follows from the definition of $\tau_k(n)$.
23. In 1984, R. Heath-Brown proved that the equality $\tau(n) = \tau(n+1)$ is true for an infinity of values of n. The sequence of numbers n such that n and $n + 1$ have the same number of divisors starts from 2, 14, 21, 26, 33, 34, 38, 44, 57, 75, 85, 86, 93, 94, 98, 104, ... (sequence A005237 in the OEIS).
24. $\sigma(n) = \sigma(n + 1)$ for $n = 14, 206, 957, 1334, 1364$ (see sequence A002961 in the OEIS).
25. More generally, $\sigma(n)$ is the total number of parts congruent to 0 modulo k in the partitions of k^n into equal parts.
26. For example, for $n = 4$, we have: one common divisor with $m = 1$, two common divisors with $m = 12$, one common divisor with $m = 3$, and one common divisor with $m = 4$. So, $\sigma(4) = 7 = 1 + 2 + 1 + 4$.
27. The first few such n are 1, 3, 7, 21, 31, 93, 127, 217, 381, 651, 889, 2667,... (sequence A046528 and the OEIS); the corresponding powers of 2 are 0, 2, 3, 5, 5, 7, 7, 8, 9, 10, 10, 12, 12, 13, 14,... (sequence A048947 in the OEIS). See [Weis22].
28. In fact, $\sigma(3^4) = 11^2$. On the other hand, Kanold (1947) shows that the equation $\sigma(q^{p-1}) = b^p$ has no solutions for $b > 2$, where q is a prime and p is an odd prime. See [Sloa22].

29. In fact, the following equalities allow us to express p and q in terms of $\sigma(n)$ and $\phi(n)$ only, without even knowing n or $p+q$:
$$\begin{aligned} p &= (\sigma(n)-\phi(n))/4 \\ &\quad - \sqrt{[(\sigma(n)-\phi(n))/4]^2 - [(\sigma(n)+\phi(n))/2-1]}, \\ q &= (\sigma(n)-\phi(n))/4 \\ &\quad + \sqrt{[(\sigma(n)-\phi(n))/4]^2 - [(\sigma(n)+\phi(n))/2-1]}. \end{aligned}$$
Also, knowing n and either $\sigma(n)$ or $\phi(n)$ (or knowing $p+q$ and either $\sigma(n)$ or $\phi(n)$) allows us to easily find p and q. See information about RSA system for practical applications.
30. Euler proved this result by logarithmic differentiation of the identity in his *pentagonal number theorem*.
31. It is easy to see that $\tau_k(n)$ is multiplicative. One can obtain this fact by induction, as $\tau_{k+1}(n) = \sum_{d|n} \tau_k(d)$. Moreover, it is easy to check that $\tau_k(p^\alpha) = \binom{\alpha+k-1}{k-1} = \frac{(\alpha+k-1)!}{(k-1)!\alpha!}$.
32. We have that
$$\sum_{n=1}^{N} \phi(n) = \sum_{n=1}^{N} n \sum_{d|n} \frac{\mu(d)}{d} = \sum_{d=1}^{N} \frac{\mu(d)}{d} \sum_{n\le N, d|n} n.$$
Using the arguments of the theorem on mean value of $\sigma(n)$ (see Chapter 2) and the formula $\sum \frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$, we obtain the result. See, for example, [Buch09].
33. See, for example, [Buch09] and [Kara83].
34. It is a generalization of the well-known *Gauss circle problem*.
35. In fact, $\mu^2(n) = \sum_{d^2|n} \mu(d)$, so
$$\begin{aligned} S(x) = |\{n \le x \mid n \text{ is square-free}\}| &= \sum_{n\le x} \mu^2(n) = \sum_{n\le x} \sum_{d^2|n} \mu(d) \\ &= \sum_{d\le\sqrt{x}} \mu(d)\left(\frac{x}{d^2} + O(1)\right) = x \sum_{d\le\sqrt{x}} \frac{\mu(d)}{d^2} + O(\sqrt{x}) \\ &= x\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O\left(\sqrt{x} + x\sum_{d>\sqrt{x}} d^{-2}\right) = \frac{x}{\zeta(2)} + O(\sqrt{x}). \end{aligned}$$
36. See the previous proof.

Solutions to Problems, Connected with Perfect Numbers

1. As $22425 \cdot \lg 2 = 22425 \cdot 0,30103\ldots = 6750,59\ldots$, then 222425 has 6751 digits, and $2^{22425} = 10^{6750}10^{0,59\ldots}$. Since $10^{0,59\ldots} > 10^{0,5} > 3$, then $10^{6751} > 2^{22425} > 3 \cdot 10^{6750}$. So, the first digit of 2^{22425} is at least 3; therefore, the number of digits will be the same after subtraction $2^{22425} - 2^{11212}$. Hence, the number $2^{11212}(2^{11213} - 1)$ has 6751 decimal digits.
2. Let $M_p = 2^p - 1$ be a Mersenne number, where p is a prime. If M_p is composite, then p is odd. By Fermat's little theorem, $\frac{M_p - 1}{2} = 2^{p-1} - 1 \equiv 0(mod\ p)$. So $\frac{M_p-1}{2} = kp$ for some positive integer k. Hence, $M_p = 2^p - 1 | (2^{kp} - 1) = 2^{\frac{M_p-1}{2}} - 1$. It is equivalent to saying that $2^{\frac{M_p-1}{2}} \equiv 1(mod\ M_p)$, which implies that $2^{M_p - 1} \equiv 1(mod\ M_p)$.
3. So, we are going to show that if $p = 2^q - 1$ is a Mersenne prime, then the congruence $2^{p-1} \equiv 1(mod\ p^2)$ does not hold.

   By Fermat's little theorem, $2^{p-1} \equiv 1(mod\ p)$. As, by definition, $p = 2^q - 1$, it holds that $2^q \equiv 1(mod\ p)$, and hence, $q|(p-1)$. Therefore, one can write $p - 1 = qk$, where $k \in \mathbb{N}$, $k \geq 2$.

   If the congruence $2^{p-1} \equiv 1(mod\ p^2)$ is satisfied, then $p^2|(2^{qk} - 1)$ and $p|\frac{2^{qk}-1}{p}$. Therefore, using that $p = 2^q - 1$, we obtain

   $$0 \equiv \frac{2^{qk} - 1}{2^q - 1} \equiv 1 + 2^q + 2^{2q} + \cdots + 2^{(k-1)q} \equiv -k(mod\ 2^q - 1).$$

   Hence, $2^q - 1|k$, and therefore, $k \geq 2^q - 1$. This leads to $p - 1 = qk \geq q(2^q - 1) = qp$, which is impossible.
4. Consider the numbers $M_{k\phi(n)} = 2^{k\phi(n)} - 1$, where $\phi(n)$ is the Euler's totient function.
5. It follows that $p_i = 2^{i-1}p_1 + (2^{i-1} - 1)$, where $p_1 = p$. By setting $a = \frac{p+1}{2}$, $p_i = 2^i a - 1$.

   Examples of (complete) Cunningham chains of the first kind include the following:

   - 2, 5, 11, 23, 47 (the next number would be 95, but that is not prime);

- 3, 7 (the next number would be 15, but that is not prime);
- 29, 59 (the next number would be $119 = 7 \cdot 17$, but that is not prime);
- 41, 83, 167 (the next number would be 335, but that is not prime);
- 89, 179, 359, 719, 1439, 2879 (the next number would be $5759 = 13 \cdot 443$, but that is not prime).

As of 2021, the longest known Cunningham chain of the first kind is of length 17, with starting prime 2759832934171386593519, discovered by J. Wroblewski in 2008.

6. It follows that $p_i = 2^{i-1}p_1 - (2^{i-1} - 1)$, where $p_1 = p$. By setting $a = \frac{p-1}{2}$, $p_i = 2^i a + 1$.
Examples of (complete) Cunningham chains of the second kind include the following:

- 2, 3, 5 (the next number would be 9, but that is not prime);
- 7, 13 (the next number would be 25, but that is not prime);
- 19, 37, 73 (the next number would be 145, but that is not prime);
- 31, 61 (the next number would be $121 = 112$, but that is not prime).

As of 2021, the longest known Cunningham chain of the second kind is of length 19, with starting prime 79910197721667870187016101, discovered by Chermoni and Wroblewski in 2014.

It has been conjectured that arbitrarily long Cunningham chains of the second kind exist.

7. See [Sloa22]. Sequence A048242 in the OEIS contains numbers that are not the sum of two abundant numbers (not necessarily distinct), with the first few members 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, … and the last member $a(1456) = 20161$. Also, $a(38) = 46$ is the largest even term. For example, $48 = 12 + 36$; $20162 = 20000 + 162$.
8. It is proven that the only even perfect number of the form x^3+1 is 28 (Makowski, 1962). Moreover, 28 is also the only even perfect

number that is a sum of two positive cubes of integers (Gallardo, 2010).

9. For example, a 7-smooth number is a number whose every prime factor is at most 7, so $49 = 7^2$ and $15750 = 2 \cdot 3^2 \cdot 5^3 \cdot 7$ are both 7-smooth, while 11 and $702 = 2 \cdot 3^3 \cdot 13$ are not 7-smooth.

   Smooth numbers are especially important in cryptography, which relies on factorization of integers. The 2-smooth numbers are just the powers of 2, while 5-smooth numbers are known as *regular numbers*.

   Berndt (1994) called the 7-smooth numbers *highly composite numbers*. In the following table, the first k-smooth numbers are represented.

k	OEIS	Numbers
2	$A000079$	$1, 2, 4, 8, 16, 32, 64, 128, 256, 512, \ldots$
3	$A003586$	$1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, \ldots$
5	$A051037$	$1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, \ldots$
7	$A002473$	$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, \ldots$
11	$A051038$	$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, \ldots$

10. The second sublime number is

$$\begin{gathered}6086555670238378989670371734243169622657830773351885970528324860512791691264\end{gathered}$$

   (see sequence A081357 in OEIS). It is not known if any odd sublime number exists.

11. The first few highly cototient numbers are 2, 4, 8, 23, 35, 47, 59, 63, 83, 89, 113, 119, 167, 209, 269, ... (sequence A100827 in the OEIS).

   Many of the highly cototient numbers are odd. In fact, after 8, all the numbers listed above are odd, and after 167, all the numbers listed above are congruent to 29 modulo 30.

12. The first few highly totient numbers are 1, 2, 4, 8, 12, 24, 48, 72, 144, 240, 432, 480, 576, 720, 1152, ... (sequence A097942 in the OEIS), with 1, 3, 4, 5, 6, 10, 11, 17, 21, 31, 34, 37, 38, 49, 54, ... totient solutions, respectively.

13. A *refactorable number* (or *tau number*) is an integer n that is divisible by the number of its divisors: $\tau(n)|n$. The first few refactorable numbers are 1, 2, 8, 9, 12, 18, 24, 36, 40, 56, 60, 72, 80, 84, 88, ... (sequence A033950 in the OEIS).

    In 2002, Zelinsky proved that no three consecutive integers can all be refactorable. Zelinsky wondered also *if there exists a refactorable number* $n_0 \equiv a (mod\ m)$, *does there necessarily exist an* $n > n_0$ *such that* n *is refactorable and* $n \equiv a (mod\ m)$. See [Zeli02].

14. For example, 18 has 6 divisors and is divisible by 6. The equation $gcd(18, x) = 6$ has infinity many solutions $x = 18k + r$, $r \in \{6, 12\}$. On the other hand, 6 has 4 divisors and is not divisible by 4. The equation $gcd(6, x) = 4$ has no solution, as 4 is not a divisor of 6.

    It is known that there are infinitely many refactorable numbers.

15. It is easy to see that numbers of the form pq and p^3 are multiplicative perfect. All such numbers have exactly three proper divisors. The first few such numbers are 6, 8, 10, 14, 15, 21, 22, 26, 27, 33, 34, 35, 38, 39, 46, ... (see sequence A030513 in the OEIS).

16. See sequence A068068 in the OEIS for the number of odd unitary divisors of $n = 1, 2, 3, \ldots$; see sequence A192066 for the sum of odd unitary divisors of $n = 1, 2, 3, \ldots$.

    The number of unitary divisors of a number n is 2^k, where k is the number of distinct prime factors of n.

17. The sum $\sigma^{**}(n)$ of the bi-unitary divisors of n (see sequence A188999 in the OEIS) is a multiplicative function with $\sigma^{**}(p^\alpha) = \sigma(p^\alpha) = \frac{p^{\alpha+1}-1}{p-1}$ for odd α and $\sigma^{**}(p^\alpha) = \sigma(p^\alpha) - p^{\alpha/2} = \frac{p^\alpha-1}{p-1}(p^{\alpha+1} + 1)$ for even α.

    In fact, $\sigma^{**}(120) = \sigma(120) = 360 = 3 \cdot 120$, so 120 is a bi-unitary 3-perfect number.

    As $\sigma^{**}(2) = 3$ and $\sigma^{**}(3) = 4$, we get that $\sigma^{**}(\sigma^{**}(2)) = 2 \cdot 2$, and 2 is a bi-unitary superperfect number. As $\sigma^{**}(9) = 10$ and $\sigma^{**}(10) = 18$, we get that $\sigma^{**}(\sigma^{**}(9)) = 2 \cdot 9$, and 9 is a bi-unitary superperfect number. T. Yamada proved that 2 and 9 are the only bi-unitary superperfect numbers.

18. Infinitary divisors can also be defined as follows. Compute the prime factorization for each divisor d of n, $d = \prod_{i=1}^{k} p_i^{\beta_i}$.

    Now, make a table of the binary representations $(\beta_i)_2$ of β_i for each prime factor p_i. The infinitary divisors are then those factors d that have zeros in the binary representation of all β_i where n itself does. This is illustrated in the following table for the number $n = 12$, which has divisors 1, 2, 3, 4, 6, and 12 and prime factors 2 and 3.

d	p_1	β_1	$(\beta_1)_2$	p_2	β_2	$(\beta_2)_2$
1	2	0	000	3	0	000
2	2	1	001	3	0	000
3	2	0	000	3	1	001
4	2	2	010	3	0	000
6	2	1	001	3	1	001
12	2	2	010	3	1	001

    As seen from the table, the divisors 1, 3, 4, and 12 have zeros in the binary expansions of β_1 (the exponents of 2) in the positions that 12 itself does. Similarly, all divisors have zeros in the leftmost two positions in the binary expansions of β_2 (the exponents of 3), as does 12 itself. The intersection of the divisors matching zero in the binary representations in each of the exponents is therefore 1, 3, 4, and 12, and these are the infinitary divisors of 12.

    One can check that the infinitary divisors of 4 are 1 and 4, while the infinitary divisors of 9 are 1 and 9. For all other $n \leq 15$, any divisor of n is its infinitary divisor. For the list of the infinitary divisors of $n = 1, 2, 3, \ldots$, see sequence A077609 in the OEIS.

    The numbers of infinitary divisors of n for $n = 1, 2, 3, \ldots$ are 1, 2, 2, 2, 2, 4, 2, 4, 2, 4, … (sequence A037445 in the OEIS).

19. For example, 2 and 2^3 are exponential divisors (e-divisors) of $8 = 2^3$, and their sum is $2+2^3 = 10$. The number of exponential divisor function $\tau^e(n)$ is multiplicative with $\tau^e(p^\alpha) = \tau(\alpha)$. The numbers of exponential divisors of $n = 1, 2, 3, \ldots$ are 1, 1, 1, 2, 1, 1, 1, 2, 2, 1, 1, 2, 1, 1, 1,… (sequence A049419 in the OEIS).

    The sum of exponential divisor function $\sigma^e(n)$ is multiplicative with $\sigma^e(p^\alpha) = \sum_{d|\alpha} p^d$. The sums of exponential divisors of $n = 1, 2, 3, \ldots$ are 1, 2, 3, 6, 5, 6, 7, 10, 12, 10, 11, 18, 13, 14, 15,… (sequence A051377 in the OEIS).

    It is easy to show that an exponential aliquot cycle will remain an exponential aliquot cycle when each member of the cycle is multiplied by a square-free number, relatively prime to every member of the cycle. So, there are an infinite number of exponential perfect numbers, of exponential amicable pairs, and of exponential sociable numbers. See, for example, [StSu74].

    If $(\beta_i + 1)|(\alpha_i + 1)$ for all $i = 1, 2, \ldots, s$, we call d a *modified exponential divisor* of n (see webpage on D. Moews). In fact, every exponential aliquot cycle can be obtained by starting with some modified exponential aliquot cycle, so looking at the number of modified exponential aliquot cycles is more interesting.
20. See [Sloa22]. For $k = 0$, we get the Euclid–Euler theorem. For $k = 1$, we get the following proposition: If $2^n - 3$ is prime (see sequence A050414 in the OEIS), then $2^{n-1}(2^n - 3)$ is a solution of the equation $\sigma(x) = 2x + 2$.
21. In fact, $24 = 1+2+3+4+6+8$. The first ten Erdős–Nicolas numbers are 24, 2016, 8190, 42336, 45864, 392448, 714240, 1571328, 61900800, and 91963648 (sequence A194472 in the OEIS). They are named after Paul Erdős and Jean-Louis Nicolas, who wrote about them in 1975.
22. As only known almost perfect number have the form 2^n, the result holds. There are 2^n subsets of an n-set. There are 2^{n-1} compositions (ordered partitions) of n.
23. In fact, $\sigma(\phi(2^{k-1} \cdot p^m)) = \sigma(2^{k-2}(p-1)p^{m-1}) = \sigma(2^{k-2}(p-1))\sigma(p^{m-1}) = \sigma(a(n))\frac{(p^m-1)}{p-1} = 4a(n)\frac{(p^m-1)}{p-1} = 2^k(p^m - 1) = 2(2^{k-1}p^m) - 2^k$. It seems that for all such equations, there exists such an infinite set of solutions.

24. For example, 24 is 5-hemiperfect because the sum of the divisors of 24 is $1+2+3+4+6+8+12+24=60=\frac{5}{2}\cdot 24$.

    In fact, 170 is the first 13-hemiperfect number, and 12 is the first 15-hemiperfect number.

25. A *harshad number* (or *Niven number*) in a given base $g \geq 2$ is an integer that is divisible by the sum of its digits when written in that base. Harshad numbers in base g are also known as g-harshad (or g-Niven) numbers. Harshad numbers were defined by D. R. Kaprekar, a mathematician from India. The word "harshad" comes from the Sanskrit *harsa* (joy) + *da* (give), meaning joy-giver. The term "Niven number" arose from a paper delivered by Niven in 1977.

    The number 18 is a harshad number in base 10 because the sum of the digits 1 and 8 is 9 $(1+8=9)$ and 18 is divisible by 9. The *Hardy–Ramanujan number* 1729 is a harshad number in base 10 since it is divisible by 19, the sum of its digits $(1729=19\cdot 91)$. The number 19 is not a harshad number in base 10 because the sum of the digits 1 and 9 is 10 $(1+9=10)$, and 19 is not divisible by 10.

    Harshad numbers in base 10 form the sequence 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 18, 20, 21, 24, ... (sequence A005349 in the OEIS).

    A number which is a harshad number in every number base is called an *all-harshad number*. There are only four all-harshad numbers: 1, 2, 4, and 6. The number 12 is a harshad number in all bases except octal.

    Many superabundant numbers, 1, 2, 4, 6, 12, 24, 36, 48, 60, 120, ..., are harshad numbers. The first exception is the 105th superabundant number, 149602080797769600. The digit sum is 81, but 81 does not divide this large number.

    Moreover, the first four superabundant numbers are all-harshad numbers: 1, 2, 4, and 6.

26. Check, for example, the numbers 15 and 39. It is proven (Mohan and Suryanarayana, 1982) that *if p is a prime number greater than 3 and $3p$ is a perfect totient number, then $p \equiv 1(mod\ 4)$.* However, not every prime p of this form leads to a perfect totient

number; for instance, $51 = 3p$, $p = 17 \equiv 1(mod\ 4)$, is not a perfect totient number.

27. In binary, $127 = 1111111_2$; in nonary, $127 = 151_9$.

    Moreover, it is a *Friedman number* in base 10 since $127 = 2^7 - 1$ as well as in binary since $1111111 = (1+1)^{111} - 1$.

    On the other hand, $5 = 101_2$ is the only Thābit number which is palindromic in binary.

Solutions to Problems, Connected with Amicable Numbers

1. In fact,

$$2^{n+1} - 1 + 2^n = 2^n(2+1) - 1 = 3 \cdot 2^n - 1,$$
$$2^{n+1} - 1 - 2^{n-1} = 2^{n-1}(4-1) - 1 = 3 \cdot 2^{n-1} - 1,$$
$$2^n(2^{n+1}(2^{n+1} + 2^{n-2}) - 1) = 2^{n+1} \cdot 2^{n-2}(8+1) = 9 \cdot 2^{2n-1} - 1.$$

2. Using simple considerations modulo 6, it is easy to check that in this case, $m \neq \sigma(n) - n$.
3. For example, if $a_1 = 2^5 = 32$, $a_2 = 2^3 \cdot 41 = 328$, then $\sigma(a_1) = 63$, $\sigma(a_2) = 630$, $A = 19026$, $B = 1134$, $R = 617893920 = 2^5 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 139$. By writing R as a product of uv, we can get

$$u = 252 = 2^2 \cdot 3^2 \cdot 7,\ v = 2451960 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 139.$$

   Then, $p = \frac{u+A}{B} = \frac{252+19026}{1134} = 17$, $q = \frac{v+A}{B} = \frac{2451960+19026}{1134} = 2179$, $s = \frac{\sigma(a-1)(p+1)(q+1)}{\sigma(a_2)} - 1 = \frac{63(18\cdot 2180}{630} - 1 = 3923$, which all are primes. So, we get an amicable pair $(M, N) = (a_1pq, a_2s) = (2^5 \cdot 17 \cdot 2179, 2^3 \cdot 41 \cdot 3923) = (1185376, 1286744)$. See [Yan96].
4. In 1968, Lee proposed this general algebraic method for constructing amicable pairs (see [Lee68] and [Yan96]). It was based on the obvious fact that an amicable pair can be written in the form $(M = a_1 \cdot p \cdot q, N = a_2 \cdot r)$, where $gcd(a_1, p) = gcd(a_1, q) = gcd(a_2, r) = 1$. Then, for given a_1, a_2, we can find unknown p, q, r. Unfortunately, it is very difficult to find a_1, a_2 such that p, q, r are integral. So, Lee's method is essentially impractical.

5. This method (see [Yan96]) is general, as any amicable pair, including exotic, could be used as a breeder pair to construct new amicable pairs. This method can be realized by the following algorithm:

   - Select a breeder pair, $(M^{'}, N^{'}) = (a_1p, a_2q)$.
   - Use (a_1, a_2) to calculate W.
   - Complete factor W into its prime decomposition form.
   - Generate all possible combinations $W = UV$ for W.
   - For each combination $W = UV, U < V$, generate q_1, q_2, p_1.
   - Test if all numbers q_1, q_2, p_1 are positive integers and primes; test if $q_1 \neq q_2$, $gcd(a_2, q_1q_2) = 1$, $gcd(a_1, p_1) = 1$; in this case, find $M = a_1p_1, N = a_2q_1q_2$.
   - Indicate (M, N) as an amicable pair.

   For example, let the breeder amicable pair be $(220, 284) = (2^2 \cdot 5 \cdot 11, 2^2 \cdot 71)$. In this case, $a_1 = 2^2 \cdot 5 = 20$, $a_2 = 2^2 = 4$, $p = 11$, $q = 71$. So, $A_1 = \sigma(a_1) = 42$, $A_2 = \sigma(a_2) = 7$, $B_1 = A_1 - a_1 = 22$, $B_2 = A_2 - a_2 = 3$, $A = a_1a_2 - B_1B_2 = 14$, $B = B_1A_2 = 154$, $C = a_1A_1 + B_1A_2 = 994$, and

   $$W = AC + B^2 = 37632 = 2^8 \cdot 3 \cdot 7^2.$$

   There are $9 \cdot 2 \cdot 3 = 54$ representations $W = UV$ of W. Select them with $U < V$, we get pairs $U = 2, V = 18816$; $U = 4, V = 9408; \ldots$; $U = 168, V = 224$; $U = 147, V = 256$. In all 26 combinations, $W = UV$ with $2 \leq U < V$, exactly two yield amicable pairs.

   For $U = 28 = 2^2 \cdot 7$, $V = 1344 = 2^6 \cdot 3 \cdot 7$, we get $(2620 = 2^2 \cdot 5 \cdot 131, 2924 = 2^2 \cdot 17 \cdot 43)$.

   For $U = 84 = 2^2 \cdot 3 \cdot 7$, $V = 448 = 2^6 \cdot 7$, we get $(5020 = 2^2 \cdot 5 \cdot 251, 5564 = 2^{\cdot}13 \cdot 107)$.

6. **I.** It is easy to see that

   $$\sigma(M) = \sigma(wpq) = \sigma(w)(p + 1)(q + 1)$$
   $$= \sigma(w)(pq + p + q + 1) = \sigma(w)(s + 1) = \sigma(ws) = \sigma(N).$$

II. From the construction, it follows that

$$p = \frac{u + \sigma(w) - w}{B} = \tfrac{u+w}{B} - 1,\ q = \tfrac{v+w}{B} - 1,$$

$$s + 1 = \frac{u+w}{B} \cdot \frac{v+w}{B} = \frac{2w^2 + w(u+v)}{B^2} = \frac{w(2w+u+v)}{B^2},$$

$$\sigma(M) = \sigma(w)(p+1)(q+1) = \sigma(w)(s+1)$$

$$= \sigma(N) = w \cdot \tfrac{\sigma(w)(2w+u+v)}{B^2},$$

$$M + N = w(pq + s) = w(2s - p - q).$$

So, $\sigma(M) = M + N$ if and only if

$$B^2(2s - p - q) = \sigma(w)(2w + u + v).$$

It is easy to see that

$$B^2(2s - p - q) = B^2 \cdot \left(\frac{2w(2w+u+v)}{B^2} - 2 - p - q\right)$$

$$= 2w(2w + u + v) - B^2(2 + p + q).$$

This is equal to $\sigma(w)(2w + u + v)$ if and only if $2w + u + v = B(p + q + 2)$, which is so if and only if

$$2w + u + v = B(p + q + 2) = B\left(\frac{u+w}{B} + \frac{v+w}{B}\right).$$

This is true, so the result follows.

For example, let $w = 2^4 = 16$. Then, $w^2 = 256$, $\sigma(w) = 31$, $A = \sigma(w) - w = 15$, $B = 2w - \sigma(w) - 1$.

Since $w^2 = 256$, it can be written in the following four ways as a product of u and v:

$$(u, v) = (2, 128), (4, 64), (8, 32), (16, 16).$$

For $(u, v) = (2, 128)$, we have $p = 2 + 15 = 17$, $q = 128 + 15 = 143 = 11 \cdot 13$, $s = 2591$; so, q is not a prime, and this case does not generate an amicable pair.

For $(u, v) = (4, 64)$, we have $p = 4 + 15 = 19$, $q = 64 + 15 = 79$, $s = 1599 = 3 \cdot 13 \cdot 41$; so, s is not a prime, and this case does not generate an amicable pair.

For $(u,v) = (8,32)$, we have $p = 8+15 = 23$, $q = 32+15 = 47$, $s = 1151$; as all q, p, s are primes, this case generates an amicable pair:

$$(M,N) = (2^4 \cdot 23 \cdot 47, 2^4 \cdot 1151) = (17296, 18416).$$

Finally, for $(u,v) = (16,16)$, we have $p = 16+15 = 31$ and $q = 16+15 = 31$; Since $q = p = 31$, this case does not generate an amicable pair.

This version of algorithm as well as the example above are represented in the book by Yan, 1996, [Yan96]. However, the ideas behind such searches go back to Euler's works. See the next problem in the list.

7. Let $w = 2^n$. Then, $w^2 = 2^{2n} = 2^x \cdot 2^{2n-x}$, $u = 2^x$, $v = 2^{2n-x}$, $A = \sigma(w) - w = 2^{n+1} - 1 - 2^n = 2^n - 1$, and $B = 2w - \sigma(w) = 2^{n+1} - (2^{n+1} - 1) = 1$. This gives the Euler's rule in which

$$p = u + A = 2^x + 2^n - 1 = 2^x(2^{n-x} + 1) - 1,$$

$$q = v + A = 2^{2n-x} + 2^n - 1 = 2^n(2^{n-x} + 1) - 1,$$

$$s = 2^{n+x}(2^{n-x} + 1)^2 - 1.$$

If $x = n - 1$, it gives the Thābit's rule, in which

$$p = 3 \cdot 2^{n-1} - 1,\ q = 3 \cdot 2^n - 1,\ s = 9 \cdot 2^{2n-1} - 1.$$

8. It is easy to see that $\sigma(M) = \sigma(wn) = \sigma(w)\sigma(m) = \sigma(w)\sigma(n) = \sigma(wn) = \sigma(N)$. On the other hand, it holds that $\sigma(M) = \sigma(w)\sigma(m) = w(m+n) = M + N$. The result is proven.

For example, let

$$(m,n) = (11\cdot 13\cdot 431\cdot 719, 127\cdot 503\cdot 809) = (44314127, 51679729).$$

Then, we have

$$\sigma(m) = \sigma(11 \cdot 13 \cdot 431 \cdot 719) = 52254720,$$

$$\sigma(n) = \sigma(127 \cdot 503 \cdot 809) = 52254720,$$

$$m + n = 95993856,\ \sigma(m) = \sigma(n) \neq m + n,$$

$$\frac{m+n}{\sigma(m)} = \frac{95993856}{52254720} = \frac{248}{135}.$$

If we select $w = 3^3 \cdot 5^2 = 675$, we get

$$gcd(m, w) = gcd(n, w) = 1,\ \sigma(w) = 1240,\ \frac{\sigma(w)}{w} = \frac{1240}{675} = \frac{248}{135}.$$

As $\frac{\sigma(w)}{w} = \frac{m+n}{\sigma(m)}$, then $(M, N) = (wm, wn)$ is an amicable pair:

$$\begin{aligned}(M = 3^3 \cdot 5^2 \cdot 11 \cdot 13 \cdot 431 \cdot 719, N = 3^3 \cdot 5^2 \cdot 217 \cdot 503 \cdot 809)\\ = (29912035715, 34883817075).\end{aligned}$$

Note that it is the case that running time of the backward method is exponential since it is based on the calculation of $\sigma(n)$ which in turn is based on complete factorization of n.

Many integers may have the same sigma value. For example, between 10^3 and 10^4, exactly 12 numbers m_i, $i = 1, 2, 3, \ldots, 12$, have $\sigma(m_i) = 3240$, So, if we can find a suitable w such that $\sigma(wm_i) = \sigma(wm_j)$, $i \neq j$, and $\frac{\sigma(w)}{w} = \frac{m_i+m_j}{\sigma(m_i)}$, then we get an amicable pair (wm_i, wm_j). In this case, the numbers w, m, n are not necessarily primes.

A detailed consideration of this algorithm can be found in [Yan96]. In Chapter 6, we presented a similar algorithm given by Yan for amicable quadruples.

9. It is the first quasi-sociable sequence, discovered by M. Dickerman in 1997. Use it for checking the following information:

$$\begin{aligned}1215571544 &= 2^3 \cdot 11 \cdot 13813313, 1270824975\\ &= 3^2 \cdot 5^2 \cdot 7 \cdot 19 \cdot 42467,\\ 1467511664 &= 2^4 \cdot 19 \cdot 599 \cdot 8059, 1530808335\\ &= 3^3 \cdot 5 \cdot 7 \cdot 1619903,\\ 1579407344 &= 2^4 \cdot 31^2 \cdot 59 \cdot 1741, 1638031815\\ &= 3^4 \cdot 5 \cdot 7 \cdot 521 \cdot 1109,\\ 1727239544 &= 2^3 \cdot 2671 \cdot 80833, 1512587175\\ &= 3 \cdot 5^2 \cdot 11 \cdot 1833439.\end{aligned}$$

10. This sequence gives the only known augmented aliquot cycle with length greater than 2 (with no others below $2 \cdot 10^{11}$), which was considered by D. Moews (2003).

    In fact, $243902764 = 2^2 \cdot 7 \cdot 23 \cdot 103 \cdot 3677$, $270193365 = 3^2 \cdot 5 \cdot 13 \cdot 31 \cdot 47 \cdot 317$, $263191852 = 2^2 \cdot 7 \cdot 11 \cdot 23 \cdot 53 \cdot 701$, $348188373 = 3^2 \cdot 13 \cdot 17 \cdot 31 \cdot 5647$, $145417011280 = 2^4 \cdot 5 \cdot 17 \cdot 43 \cdot 2486611$, $220890775665 = 3 \cdot 5 \cdot 7 \cdot 947 \cdot 2221459$, $183450487696 = 2^4 \cdot 7^3 \cdot 359 \cdot 93113$, $232210408305 = 3 \cdot 5 \cdot 61 \cdot 253781867$.
11. It turn out that the classical Euler's method for amicable pairs of the form (apq, as) can be generalized to aliquot $2k$-cycles. This generalization for quadruples is due to Borho.

    For p_i and q_i to be integers, a necessary condition is

    $$(a_1 - a_2)(\sigma(a_1)\sigma(a_2)) \equiv 0(mod\ (a_1a_2 - s(a_1)s(a_2))).$$

    The following two quadruples are aliquot 4-cycles:

    $$(28158165, 29902635, 30853845, 2997155);$$

    $$(2387776550, 2497625050, 2550266150, 2506553050).$$

    They are each in the above form with $a_1 = 3^3 \cdot 5 \cdot 7$, $d_1 = 3^2 \cdot 5 \cdot 7$, $p - 1 = 83$, $p_2 = 359$, $r = 31643$, $a_2 = 3^3 \cdot 5 \cdot 11$, $d_2 = 3^4 \cdot 5 \cdot 11$, $q_1 = 79$, $q_2 = 263$, $t = 20183$ for the first cycle and with $a_1 = 2 \cdot 5^2 \cdot 19 \cdot 31$, $d_1 = 2 \cdot 5^3 \cdot 31$, $p_1 = 89$, $p_2 = 911$, $r = 84809$, $a_2 = 2 \cdot 5^2 \cdot 31 \cdot 59$, $d_2 = 2 \cdot 5 \cdot 19 \cdot 31 \cdot 59$, $q_1 = 79$, $q_2 = 353$, $t = 27409$ for the second.
12. This method is a particular case of the above algorithm applied for the special choice of a_1 and a_2. See also Chapter 6.
13. Cycles in $G_{n,s}$ represent sociable numbers within the interval $[1, n]$. Two special cases are loops that represent perfect numbers and cycles of length two that represent amicable pairs.
14. Use the definition of a reduced amicable pair.
15. Use the definition of an augmented amicable pair.

This page intentionally left blank

Bibliography

[AbSt72] Abramowitz M. and Stegun I.A. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, New York: Dover Publications (1972).

[AkFr09] Akbary A. and Friggstad Z. Superabundant numbers and the Riemann hypothesis, *Am. Math. Mon.*, 116(3), 273–275, (2009).

[AOS67] Alanen J., Ore O. and Stemple J. Systematic computations of amicable numbers, *Math. Comp.* 21, 98, 242–245, (1967).

[AlEr44] Alaoglu L. and Erdős P. On highly composite and similar numbers, *Trans. Am. Math. Soc.*, 56(3), 448–469, (1944).

[AGP94] Alford W.R., Granville A. and Pomerance C. There are infinitely many Carmichael numbers, *Ann. Math.*, 139, 703–722, (1994).

[Andr98] Andrews G.E. *The Theory of Partitions*, Cambridge, England: Cambridge University Press (1998).

[Apos86] Apostol T.M. *Introduction to Analytic Number Theory*, Springer-Verlag: New-York (1986).

[Arno38] Arnold I.V. *Theoretical Arithmetics*, Moscow: Uchpedgiz, (1938).

[Avan67] Avanesov E.T. Solution of a problem on figurate numbers, *Acta Arith.*, 12, 409–420, (1967).

[BaCo87] Ball W.W.R. and Coxeter H.S.M. *Mathematical Recreations and Essays*, 13th ed., New York: Dover (1987).

[BSW89] Bateman P.T., Selfridge J.L. and Wagstaff Jr. S.S. The new Mersenne conjecture, *Am. Math. Mon., Math. Assoc. Am.*, 96(2), 125–128, (1989).

[BaBo88] Battiato S. and Borho W. Are there odd amicable numbers not divisible by three? *Math. Comp.*, 50, 633–637, (1988).

[BeEr74] Benkoski S. and Erdős P. On weird and pseudoperfect numbers, *Math. Comp.*, 28(126), 617–623, (1974).

[BiBa70] Birkhoff G. and Bartee T.C. *Modern Applied Algebra*, New York: McGraw Hill Text (1970).

[Bond93] Bondarenko B.A. *Generalized Pascal's Triangles and Pyramids, Their Fractals, Graphs, and Applications*, Fibonacci Association, p. 279, (1993).

[Borh69] Borho W. Über die Fixpunkte der k-fach iterierten Teilersummenfunktion, *Mitt. Math. Gesellsch.*, Hamburg, 9, 34–48, (1969).

[Borh72] Borho W. On Thābit ibn Kurrah's formula for amicable numbers, *Math. Comp.*, 26(118), 571–578, (1972).

[Borh74] Borho W. Eine Schrancke für Befreundete Zahlen mit gegebener Teileranzahl, *Math. Nachr.*, 63, 297–301, (1974).

[BoHo86] Borho W. and Hoffmann Y. Breeding amicable numbers in abundance, *Math. Comp.*, 46, 281–293, (1986).

[Bras88] Brassard G. *Modern Cryptology*, New York: Springer-Verlag (1988).

[BrMc68] Bratley P. and McKay J. More amicable numbers, *Math. Comp.*, 22, 677–678, (1968).

[BLM70] Bratley P., Lunnon F. and McKay J. Amicable numbers and their distribution, *Math. Comp.*, 24, 431–432, (1970).

[Brow39] Brown B.H. A new pair of amicable numbers, *Am. Math. Mon.*, 46, 345, (1939).

[BAAS73] Brown E., Abbott H., Aull C. and Suryanarayana D. Quasiperfect numbers, *Acta Arith.*, 22(4), 439–447, (1973).

[BrSc95] Browkin J. and Schinzel A. On integers not of the form $n-\phi(n)$, *Colloq. Math.,* 68(1), 55–58, (1995).

[Buch09] Buchstab A.A. *Number Theory*, Moscow: Lan (2009).

[BePa01] Burnett S. and Paine S. *RSA Security's Official Guide to Gryptography*, New York: Osborne/McGraw-Hill (2001).

[Call92] Callan D. Solution to problem 6616, *Am. Math. Mon.*, 99, 783–789, (1992).

[Cata88] Catalan E. Propositions et questions diverses, *Bull. Soc. Math. de France*, 16, 128–129, (1887–1888).

[Catt51] Cattaneo P. Sui numeri quasiperfetti, *Boll. Un. Mat. Ital. Ser. 3*, 6, 59–62, (1951).

[Chan70] Chandrasekharan K. *Arithmetical Functions*, Berlin-Heidelberg: Springer-Verlag (1970).

[ChZh11] Chen Y.-G. and Zhao Q.-Q. Nonaliquot numbers, *Publ. Math. Debrecen*, 78(2), 439–442, (2011).

[Cher39] Chernick J. On Fermat's simple theorem, *Bull. Am. Math. Soc.*, 45(4), 269–274, (1939).

[Clar13] Clark R.A. Gaussian amicable pairs, Online Theses and Dissertations, p. 158 (2013).

[Cohe60] Cohen E. The number of unitary divisors of an integer, *Am. Math. Mon.*, 67(9), 879–880, (1960).

[CoWi85] Cohen G.L. and Williams R.J. Extensions of some results concerning odd perfect numbers, *Fibonacci Q.*, 23(1), 70–76, (1985).

[Cohe87] Cohen G.L. On the largest component of an odd perfect number, *J. Aust. Math. Soc., Ser. A*, 42(2), 280–286, (1987).

[Cohe90] Cohen G.L. On an integers' infinitary divisors, *Math. Comp.*, 54(189), 395–411, (1990).

[CGH95] Cohen, G.L., Gretton S. and Hagis P. Jr. Multiamicable numbers, *Math. Comp.*, 64, 212, 1743–1753, (1995).

[CoRi96] Cohen G.L. and te Riele H.J.J. Iterating the sum-of-divisors function, *Exp. Math.*, 5(2), 93–100, (1996).

[Cohe97] Cohen G.L. Numbers whose positive divisors have small integral harmonic mean, *Math. Comp.*, 66, 883–891, (1997).

[Cohe70] Cohen H. On amicable and sociable numbers, *Math. Comp.*, 24(110), 423–429, (1970).

[Cohe93] Cohen H. *A Course in Computational Algebraic Number Theory*, New York: Springer-Verlag (1993).

[Cohn65] Cohn J.H.E. Lucas and Fibonacci numbers and some Diophantine equations, *Proc. Glasgow Math. Assn.*, 7, 24–28, (1965).

[Colt99] Colton S. Refactorable numbers – A machine invention, *J. Integer Sequences*, 2, Article 99.1.2, (1999).

[CoGu96] Conway J.H. and Guy R.K. *The Book of Numbers*, New York: Springer-Verlag (1996).

[CoKe90] Cooper C.N. and Kennedy R.E. Tau numbers, natural density, and Hardy and Wright's theorem 437, *Int. J. Math. Math. Sci.*, 13, 383–386, (1990).

[Cost78] Costello P. Amicable pairs of Euler's first form, *J. Rec. Math.*, 10, 183–189, (1977–1978).

[CoRo96] Courant R. and Robbins H. *What is Mathematics? An Elementary Approach to Ideas and Methods*, 2nd ed., Oxford, England: Oxford University Press (1996).

[CuWu17] Cunningham A.J.C. and Woodall H.J. Factorisation of $Q = (2^q \mp q)$ and $(q \cdot 2^q \mp 1)$, *Messenger Math.*, 47, 1–38, (1917).

[Dave47] Davenport H. The geometry of numbers, *Math. Gaz.*, 31, 206–210, (1947).

[Dave99] Davenport H. *The Higher Arithmetic: An Introduction to the Theory of Numbers*, 8th ed., Cambridge, England: Cambridge University Press (2008).

[Dede63] Dedekind R. *Essays on the Theory of Numbers*, Cambridge, England: Cambridge University Press (1963).

[Dele98] Deléglise M. Bounds for the density of abundant integers, *Exp. Math.*, 7(2), 137–143, (1998).

[DeMo10] Deza E. and Model D. *Elements of Discrete Mathematics*, Moscow: URSS (2010).

[DeDe12] Deza E. and Deza M.M. *Figurate Numbers*, World Scientific (2012).

[DeKo13] Deza E.I. and Kotova L.V. *Collection of Problems on Number Theory*, Moscow: URSS (2013).

[Deza17] Deza E. *Special Positive Integer Numbers*, Moscow: URSS (2017).

[Deza18] Deza E. *Special Combinatorial Numbers*, Moscow: URSS (2018).

[DeKo18] Deza E.I. and Kotova L.V. *Introduction into Cryptography*, Moscow: URSS (2018).

[Deza21] Deza E.I. *Mersenne Numbers and Fremat Numbers*, World Scientific (2021).

[Dick11] Dickson L.E. All positive integers are sums of values of a quadratic function of x, *Bull. Am. Math. Mon.*, 18, p. 109, (1911).

[Dick13a] Dickson L.E. Amicable number triples, *Am. Math. Mon.*, 20, 84–92, (1913).

[Dick13] Dickson L.E. Theorems and tables on the sum of the divisors of a number, *Quarterly J. Math.*, 44, 264–296, (1913).

[Dick27] Dickson L.E. All positive integers are sums of values of a quadratic function of x, *Bull. Am. Math. Soc.*, 33, 713–720, (1927).

[Dick05] Dickson L.E. *History of the Theory of Numbers*, New York: Dover (2005).

[DiHe76] Diffie W. and Hellman M.E. New directions in cryptography, *Trans. Inf. Theory*, 22(6), 644–654, (1976).

[Diop74] Diophantus. *Arithmetics and the Book of Polygonal Numbers*, Moscow: Nauka (1974).

[DiDe63] Dirichlet J.P.G.L. and Dedekind R. *Vorlesungen Über Zahlentheorie*, F. Vieweg und sohn (1863).

[Ehrm67] Ehrman J.R. The number of prime divisors of certain Mersenne numbers, *Math. Comp.*, 21(100), 700–704, (1967).

[Erdo34] Erdős P. On the density of the abundant numbers, *J. London Math. Soc.*, 9, 278–282, (1934).

[ErOb37] Erdős P. and Obláth R. Über diophantische Gleichungen der Form $n! = x^p \pm y^p$ und $n! \pm m! = x^p$, *Acta Szeged.*, 8, 241–255, (1937).

[Erdo55] Erdős P. On amicable numbers, *Publicationes Mathematicae Debrecen*, 4, 108–111, (1955).

[Erdo73] Erdős P. Über die Zahlen der form $\sigma(n) - n$ und $n - \phi(n)$, *Elemente der Math.*, 28, 83–86, (1973).

[Erdo76] Erdős P. On asymptotic properties of Aliquot sequences, *Math. Comp.*, 30, 641–645, (1976).

[ErNi75] Erdős P. and Nicolas J.L. Repartition des nombres superabondants, *Bull. Soc. Math. France*, 103, 65–90, (1975).

[Esco46] Escott E.B.E. Amicable numbers, *Scripta Math.*, 12, 61–72, (1946).

[Eule48] Euler L. Introductio in analysin infinitorum, 1, 2, *Marc Michel Bousquet* (1748).

[Eule50] Euler L. De Numeris Amicabilibus, In *Opera Omnia, Series Prima*, Vol. 2. Leipzig, Germany: Teubner (1915).

[FNO12] Fletcher S.A., Nielsen P.P. and Ochem P. Sieve methods for odd perfect numbers, *Math. Comp.*, 81(279), 1753–1776, (2012).

[Flam91] Flammenkamp A. New sociable numbers, *Math. Comp.*, 56, 194, 871–873, (1991).

[FlLu00] Flammenkamp A. and Luca F. Infinite families of noncototients, *Colloq. Math.*, 86(1), 37–41, (2000).

[Ford99] Ford K. The number of solutions of $\phi(x) = m$, *Ann. Math.*, 150(1), 283–311, (1999).

[Gall10] Gallardo L.H. On a remark of Makowski about perfect numbers, *Elem. Math.*, 65, 121–126, (2010).

[Gard61] Gardner M. *Second Book of Mathematical Puzzles and Diversions*, W.N. Freeman, New York (1961).

[Gard68] Gardner M. A short treatise on the useless elegance of prefect numbers and amicable pairs, *Sci. Am.*, 218, 121–126, (1968).

[Gard78] Gardner M. Perfect, amicable, sociable, Ch. 12, In *Mathematical Magic Show: More Puzzles, Games, Diversions, Illusions and Other Mathematical Sleight-of-Mind from Scientific American*, New York: Vintage (1978).

[Gard88] Gardner M. *Time Travel and Other Mathematical Bewilderments*, New York: Freeman (1988).

[Gard89] Gardner M. *Penrose Tiles to Trapdoor Ciphers*, New York: W.N. Freeman (1989).

[Garc54] García M. On numbers with integral harmonic mean, *Am. Math. Mon.*, 61, 89–96, (1954).

[Garc57] García M. New amicable pairs, *Scripta Mathematica*, 23, 1–4, 167–171, (1957).

[Garc92] García M. Favorable conditions for amicability, *J. Recr. Math.*, 24, 245–249, (1992).

[Garc03] García M. The first known type $(7, 1)$ amicable pair, *Math. Comp.*, 72, 939–940, (2003).

[Gaus01] Gauss C.F. *Disquisitiones Arithmeticae*, Leipzig (1801).

[GPR03] García M., Pedersen J.M. and te Riele H.J.J. Amicable pairs, a survey, Report MAS-R0307 (2003).

[Gees20] De Geest P. Palindromic numbers and other recreational topics, (Accessed 29 January 2022). http://www.worldofnumbers.com/.

[Gelf98] Gelfand I.M. *Lectures on Linear Algebra*, Mineola, New-York: Courier Dover Publications (1998).

[Gera06] Gerardin A.M. Sur la determination des Nombres amicables, *Mathesis*, 26, (1906).

[GIMPS20] Great Internet Mersenne Prime Search (GIMPS). (Accessed 29 January 2022). https://ru.wikipedia.org/wiki/GIMPS.

[Gill64] Gillies D.B. Three new Mersenne primes and a statistical theory, *Math. Comp.*, 18(85), 93–97, (1964).

[GKP94] Graham R.L., Knuth D.E. and Patashnik O. *Concrete Mathematics: A Foundation for Computer Science*, 2nd ed., Reading, MA: Addison-Wesley (1994).

[Guy94] Guy R.K. *Unsolved Problems in Number Theory*, 2nd ed., New York: Springer-Verlag (1994).

[Hagi70] Hagis P. Jr. Lower bounds for relatively prime amicable pairs of opposite parity, *Math. Comp.*, 24, 963–968, (1970).

[Hagi75] Hagis P. Jr. On the number of prime factors of a pair of relatively prime amicable numbers, *Math. Mag.*, 48, 263–266, (1975).

[HaMc72] Hagis P. Jr. and McDaniel W.L. A new result concerning the structure of odd perfect numbers, *Proc. Am. Math. Soc.*, 32(1), 13–15, (1971).

[HaLo77] Hagis P. and Lord G. Quasi-amicable numbers, *Math. Comp.*, 31, 138, 608–611, (1977).

[HaCo82] Hagis P. Jr. and Cohen G.L. Some results concerning quasiperfect numbers, *J. Aust. Math. Soc., Ser. A*, 33, 275–286, (1982).

[HaWr79] Hardy G.H. and Wright E.M. *An Introduction to the Theory of Numbers*, 5th ed., Oxford, England: Clarendon Press (1979).

[Hogg69] Hoggatt V.E. Jr. *The Fibonacci and Lucas Numbers*, Boston, MA: Houghton Mifflin (1969).

[Hons91] Honsberger R. *More Mathematical Morsels*, Washington, DC: Mathematical Association of America (1991).

[Hool76] Hooley C.H. *Applications of Sieve Methods*, Cambridge Tracts in Mathematics, 70, Cambridge University Press (1976).

[JoLo99] Jones C.H. and Lord N. Characterising non-trapezoidal numbers, *Math. Gaz.*, 83(497), 262–263, (1999).

[John77] Johnson A.W. Absolute primes, *Math. Mag.*, 50, 100–103, (1977).

[Ingh32] Ingham A. *The Distribution of Prime Numbers*, Cambridge, England: Cambridge University Press (1932).

[IrRo90] Ireland K. and Rosen M. *A Classical Introduction to Modern Number Theory*, New York: Springer-Verlag (1990).

[Ivic85] Ivić A. *The Riemann Zeta Function*, New York: John Wiley & Sons (1985).

[Kahn67] Kahn D. *The Codebreakers – The Story of Secret Writing*, New York: Charles Scribner's Sons (1967).

[Kano50] Kanold H.-J. Satze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretisehe Probleme. II, *J. für die reine und angewandte Mathematik*, 188(1), 129–146, (1950).

[Kano53] Kanold H.-J. Über befreundete Zahlen, I, II, *Math. Nachr.,* 9, 10, 243–248, 99–111, (1953).

[Kano56] Kanold H.J. Eine Bemerkung über die Menge der vollkommenen zahlen, *Math. Ann.,* 131(4), 390–392, (1956).

[Kano57] Kanold H.J. Über das harmonische Mittel der Teiler einer naturlichen Zahl, *Math. Ann.*, 133, 371–374, (1957).

[Kerc83] Kerckhoffs A. La cryptographie militaire, *J. des Sciences Militaires*, 9, 5–38, (1983).

[Kara83] Karatsuba A.A. *Basic Analytic Number Theory*, Moscow: Nauka (1983).

[KaVo92] Karatsuba A.A. and Voronin S.M. *The Riemann Zeta-function*, Berlin: Walter de Gruyter & Co. (1992).

[Kell95] Keller W. New Cullen primes, *Math. Comput.*, 64(212), 1733–1741, (1995).

[Khin97] Khinchin A. *Continued Fractions*, Mineola, New-York: Dover Publications (1997).

[Knut68] Knuth D.E. *Fundamental Algorithms*, Bonn: Addison-Wesley (1968).

[Knut76] Knuth D.E. Mathematics and computer science. Coping with finiteness, *Science*, 194(4271), 1235–1242, (1976).

[KGP94] Knuth D., Graham R. and Patashnik O. *Concrete Mathematics: A Foundation for Computer Science*, Bonn: Addison-Wesley (1994).

[Kobl87] Koblitz N. *A Course in Number Theory and Cryptography*, Graduate Texts in Math., 114, New York: Springer-Verlag (1987).

[KoIv96] de Koninck J.M. and Ivić A. On a sum of divisors problem, *Publications de l'Institut Mathematique*, 64(78), 9–20, (1996).

[Koni09] de Koninck J.M. *Those Fascinating Numbers*, Canada: AMS Bookstore (2009).

[Kost82] Kostrikin A. *Introduction to Algebra*, New York: Springer Verlag (1982).

[Krav75] Kravitz S. Corrigendum: On weird and pseudoperfect numbers, *Math. Comp.*, 29, 673–674, (1975).

[Krav76] Kravitz S. A search for large weird numbers, *J. Recr. Math.*, 9, 82–85, (1976).

[KLS01] Krízek M., Luca F. and Somer L. 17 *Lectures on Fermat Numbers: From Number Theory to Geometry*, CMS Books in Mathematics, 9, New York: Springer-Verlag (2001).

[Laga02] Lagarias J.C. An elementary problem equivalent to the Riemann hypothesism, *Am. Math. Mon.*, 109, 534–543, (2002).

[Lagr70] Lagrange J.L. Démonstration d'un Téorème d'Arithmétique, Nouveaux Mémoires de l'Acad. Royale des Sci. et Belles-L. de Berlin (1770).

[Land09] Landau E. *Handbuch der Lehre von der Verteilung der Primzahlen*, Leipzig, Berlin: Teubner (1909).

[Lee68] Lee E.J. Amicable numbers and the bilinear diophantine equation, *Math. Comp.*, 22, 101, 181–187, (1968).

[Lee69] Lee E.J. On divisibility by nine of the sums of even amicable numbers, *Math. Comp.*, 23, 107, 545–548, (1969).

[LeMa72] Lee E.J. and Madachy J.S. The history and discovery of amicable numbers, *J. Recreational Math.*, 5, part 1, 77–93, part 2, 153–173, part 3, 231–249, (1972).

[Lege79] Legendre A.-M. *Théorie des Nombres*, 4th ed., Paris: A. Blanchard (1979).

[LiNi96] Lidl R. and Niederreiter H. *Finite Fields*, Cambridge, England: Cambridge University Press (1996).

[Line86] Lines M.E. *A Number for Your Though*, Bristol: Adam Hilger (1986).

[LeLi83] Le Lionnais F. *Les Nombres Remarquables*, Paris: Hermann (1983).

[Luca75] Lucas É. Question 1180, *Nouv. Ann. Math., Ser. 2*, 14, 429–432, (1875).

[Luca00] Luca F. The anti-social Fermat number, *Am. Math. Mon.*, 107(2), 171–173, (2000).

[Luca01] Luca F. Fermat numbers in the Pascal's triangle, *Divulgaciones Matemáticas*, 9(2), 191–195, (2001).

[Mada79] Madachy J.S. *Madachy's Mathematical Recreations*, New York: Dover (1979).

[Mako92] Makowski A. Remark on perfect numbers, *Elem. Math.*, 17(5), 109, (1962).

[Malc86] Malcolm E. *A Number for Your Thoughts: Facts and Speculations about Number from Euclid to the Latest Computers*, Boca Raton, Florida: CRC Press (1986).

[Maso21] Mason T.E. On amicable numbers and their generalisations, *Am. Math. Mon.*, 28(5), 195–200, (1921).

[MaSt15] Mazur B. and Stein W. *Prime Numbers and the Riemann Hypothesis*, Cambridge, England: Cambridge University Press (2015).

[McDa70] McDaniel W.L. The non-existence of odd perfect numbers of a certain form, *Archiv der Mathematik.*, 21(1), 52–53, (1970).

[McDa74] McDaniel W.L. Perfect Gaussian integers, *Acta Arith.*, XXV, 137–144, (1974).

[McHa75] McDaniel W.L. and Hagis P. Jr. Some results concerning the non-existence of odd perfect numbers of the form $p^{\alpha}M^{2\beta}$, *Fibonacci Quarterly*, 13(1), 25–28, (1975).

[Melf95] Melfi G. A survey on practical numbers, *Rend. Sem. Mat. Univ. Pol. Torino*, 53(4), 347–359, (1995).

[Melf96] Melfi G. On two conjectures about practical numbers, *J. Number Theory*, 56(1), 205–210, (1996).

[Melf15] Melfi G. On the conditional infiniteness of primitive weird numbers, *J. Number Theory*, 147, 508–514, (2015).

[MSC96] Mitrinovic D.S., Sándor J. and Crstici B. *Handbook on Number Theory*, Kluwer Academic Publishers (1996).

[MoMo91] Moews D. and Moews P.C. A search for aliquot cycles below 10^{10}, *Math. Comp.*, 57, 849–855, (1991).

[MoMo93] Moews D. and Moews P.C. A search for aliquot cycles and amicable pairs, *Math. Comp.*, 61, 935–938, (1993).

[Moto83] Motohashi Y. *Lectures on Sieve Methods and Prime Number Theory*, Berlin: Springer-Verlag (1983).

[Moze09] Mozer L. *An Introduction to the Theory of Numbers*, The Trillia Group West Lafayette, IN (2009).

[Nank79] Nankar M.L. History of perfect numbers, *Ganita Bharati,* 1, 1–2, (1979).

[Nage51] Nagell T. *Introduction to Number Theory*, New York: Wiley (1951).

[Nage61] Nagell T. The Diophantine equation $x^2 + 7 = 2^n$, *Ark. Mat.*, 30, 185–187, (1961).

[Niel03] Nielsen P.P. An upper bound for odd perfect numbers, *Integers*, 3, A14–A22, (2003).

[Nico69] Nicolas J.-L. Ordre maximal d'un elément du groupe S_n des permutations et "highly composite numbers", *Bull. Soc. Math. France*, 97, 129–191, (1969).

[Niel07] Nielsen P.P. Odd perfect numbers have at least nine distinct prime factors, *Math. Comp.*, 76(260), 2109–2126, (2007).

[Nico26] Nicomachus of Geraza. *Introduction in Arithmetic*, Translated by Martin Luther D'Ooge, Macmillan (1926).

[OcRa12] Ochem P. and Rao M. Odd perfect numbers are greater than 10^{1500}, *Math. Comp.*, 81(279), 1869–1877, (2021).

[Ore48] Ore O. *Number Theory and its History*, Mineola, New-York: Dover Publications, Inc. (1948).

[Ore48a] Ore O. On the averages of the divisors of a number, *Am. Math. Mon.*, 55(10), 615–619, (1948).

[Pasc54] Pascal B. *Traité du triangle arithmétique, avec quelques autres petits traitez sur la mesme matière*, Paris: Guillaume Desprez (1654).

[PeBy70] Pettofrezzo A.J. and Byrkit D.R. *Elements of Number Theory*, Englewood Cliffs: Prentice Hall (1970).

[Pier95] Pierpont J. On an undemonstrated theorem of the Disquisitiones Arithmetica, *Bull. Am. Math. Soc.*, 2(3), 77–83, (1895).

[Pill43] Pillai S.S. Highly abundant numbers, *Bull. Calcutta Math. Soc.*, 35, 141–156, (1943).

[Plou92] Plouffe S. *1031 Generating Functions and Conjectures*, Québec – Montréal: Université du Québec à Montréal (1992).

[Plut78] Plutarch. Platonic questions, in *The Morals*, Vol. 5, Boston: Little, Brown, and Co. (1878).

[Poll74] Pollard J.M. Theorems on factorization and primality testing, *Proc. Cambridge Phil. Soc.*, 76, 521–528, (1974).

[Pome73] Pomerance C. Abstract 709-A5, *Notices Am. Math. Soc.*, 20, A-648, (1973).

[Pome77] Pomerance C. On the distribution of amicable numbers, *J. Reine Angew. Math.*, 293/294, 217–222, (1977).

[Pome81] Pomerance C. On the distribution of amicable numbers, II, *J. Reine Angew. Math.*, 325, 182–188, (1981).

[PoLu10] Pomerance C. and Luca F. On the radical of a perfect number, *New York J. Math.*, 16, 23–30, (2010).

[Poul18] Poulet P. *Parfaits, Amicables et Extensions,* Bruxelles: Editions Stevens (1918).

[Poul18a] Poulet P. Question 4865, *L'intermed. des Math.*, 25, 100–101, (1918).

[Poul29] Poulet P. *La Chasse aux Nombres*, Brussels: Fascicule I (1929).

[Poul48] Poulet P. 43 new couples of amicable numbers, *Scripta Mathematica*, 14, 1, 77, (1948).

[Prim22] The Prime Pages (prime number research, records and resources). (Accessed 29 January 2022). https://primes.utm.edu/.

[RaTo57] Rademacher H. and Toeplitz O. *The Enjoyment of Mathematics: Selections from Mathematics for the Amateur*, Princeton, NJ: Princeton University Press (1957).

[Rama15] Ramanujan S. Highly composite numbers, *Proc. London Math. Soc. Series 2*, 14, 347–409, (1915).

[Rama00] Ramanujan S. *Collected Papers of Srinivasa Ramanujan*, Hardy G.H., Aiyar P.V.S. and Wilson B.M. (eds.), Providence, RI: American Mathematical Society (2000).

[Ribe89] Ribenboim P. *The Book of Prime Number Records*, New York: Springer-Verlag (1989).

[Ribe96] Ribenboim P. *The New Book of Prime Numbers Records*, New-York: Springer-Verlag (1996).

[Riel74] te Riele H.J.J. Four large amicable pairs, *Math. Comp.*, 28, 105, 309–312, (1974).

[Riel84] te Riele H.J.J. New very large amicable pairs, Number Theory, Noordwijkerhout (1983); Springer Lecture Notes in Mathematics 1068, 210–215, (1984).

[Riel84a] te Riele H.J.J. On generating new amicable pairs from given amicable pairs, *Math. Comp.*, 42, 165, 219–223, (1984).

[Riel86] te Riele H.J.J. Computation of all amicable pairs below 10^{10}, *Math. Comp.*, 47, 175, 361–368, (1986).

[Ries94] Riesel H. *Prime Numbers and Computer Methods for Factorization*, 2nd ed., Basel: Birkhouser (1994).

[Robe08] Roberts T. On the form of an odd perfect number, *Aust. Math. Gaz.*, 35(4), 244, (2008).

[Robi84] Robin G. Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann, *J. de Mathématiques Pures et Appliquées, Neuvieme Serie*, 63(2), 187–213, (1984).

[Rolf65] Rolf H.L. Friendly numbers, *Am. Math. Mon.*, 72, 4, 455, (1965).

[Rolf67] Rolf H.L. Friendly numbers, *Math. Teachers*, 60, 2, 157–160, (1967).

[Salo90] Salomaa A. *Public-Key Cryptography*, Berlin-Heidelberg: Springer-Verlag (1990).

[Seeh84] Seehoff P. Befreundete Zahlen, *Hoppe Archiven*, 70, 75–90, (1884).

[Shan93] Shanks D. *Solved and Unsolved Problems in Number Theory*, 4th ed., New York: Chelsea (1993).

[Sier55] Sierpiński W. Sur une propriete des nombres naturels, *Annali di Matematica Pura ed Applicata*, 39(1), 69–74, (1955).

[Sier64] Sierpiński W. *Elementary Theory of Numbers*, Warszawa: Państwowe Wydawn, Naukowe: Państwowe Wydawn, Naukowe (1964).

[Sing00] Singh S. *The Code book: The Secret History of Codes and Code-breaking*, London: Forth Estate (2000).

[SlPl95] Sloane N.J.A. and Plouffe S. *The Encyclopedia of Integer Sequences*, San Diego: Academic Press (1995).

[Sloa22] Sloane N.J.A. at all On-line encyclopedia of integer sequences. http://oeis.org/ 29.01.2022.

[Smal02] Smallbone K. *Perfect Numbers Over Simple Algebraic Number Fields* (2002).

[Smit84] Smith D.E. *A Source Book in Mathematics*, New York: Dover (1984).

[Smit97] Smith J. Trapezoidal numbers, *Math. School*, 11, 46–47, (1997).

[Spir18] Spira R. The complex sum of divisors, *Am. Math. Mon.*, 68, 2, 120–124, (2018).

[Stau40] von Staudt K.G.Ch. Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffend, *J. fur die reine und angewandte Mathematik*, 21, 372–374, (1840).

[Step01] Stepanova L.L. *Selected Chapters in Number Theory*, Moscow: MSPU (2001).

[Stra16] Strang G. *Linear Algebra and its Applications*, 5th ed., Wellesley-Cambridge Press (2016).

[StSu74] Straus E.G. and Subbarao M.V. On exponential divisors, *Duke Math. J.*, 41, 465–471, (1974).

[Stew54] Stewart B.M. Sums of distinct divisors, *Am. J. Math.*, 76(4), 779–785, (1954).

[Stru87] Struik D.J. *A Concise History of Mathematics*, Dover Publications (1987).

[Sury69] Suryanarayana D. Super perfect numbers, *Elem. Math.*, 24, 16–17, (1969).

[Titc87] Titchmarsh E.Ch. *The Theory of the Riemann Zeta-Function*, 2nd ed., Oxford University Press (1987).

[Uspe76] Uspensky V.A. *Pascal's Triangle: Certain Applications of Mechanics to Mathematics*, Moscow: Mir (1976).

[Vile14] Vilenkin N.Ia. *Combinatorics*, Moscow: Academic Press (2014).

[Vino03] Vinogradov I.M. *Elements of Number Theory*, Mineola, NY: Dover Publications (2003).

[Voro61] Vorob'ev N.N. *Fibonacci Numbers*, New York: Blaisdell (1961).

[Wall72] Wall C.R. Bi-unitary perfect numbers, *Proc. Am. Math. Soc.*, 33, 39–42, (1972).

[Wall75] Wall C.R. The fifth unitary perfect number, *Canad. Math. Bull.*, 18, 115–122, (1975).

[Want36] Wantzel M.L. Recherches sur les Moyens de Reconnaître si un Problème de Géométrie Peut se Pésoudre avec la Règle et le Compas, *J. Math. Pures Appliq.*, 1, 366–372, (1836).

[Weis99] Weisstein E.W. *CRC Concise Encyclopedia of Mathematics*, Boca Raton, Florida: CRC Press (1999).

[Weis22] Weisstein E.W. MathWorld – A Wolfram web resource. (Accessed 29 January 2022). http://mathworld.wolfram.com/.

[Well86] Wells D. *The Penguin Dictionary of Curious and Interesting Numbers*, Middlesex: Penguin Books (1986).

[Wief09] Wieferich A. Beweis des Satzes, dass sich eine jede ganze Zahl als Summe von höchstens neun positiven Kuben darstellen lässt, *Math. Ann.*, 66, 95–101, (1909).

[Wiet88] Wiethaus H. Über befreundete Zahlen, Master's thesis, Dortmund (1988).

[Wiki22] Wikipedia, the free Encyclopedia. (Accessed 29 January 2022). http://en.wikipedia.org.

[Yama19] Yamada T. A new upper bound for odd perfect numbers of a special form, *Colloquium Mathematicum*, 156(1) (2019).

[Yan94] Yan S.Y. 68 new large amicable pairs, *Comp. Math. App.*, 28, 5, 71–74, (1994).

[Yan96] Yan S.Y. *Perfect, Amicable and Sociable Numbers. A Computational Approach*, World Scientific (1996).

[Zeli02] Zelinsky J. Tau numbers: A partial proof of a conjecture and other results, *J. Integer Sequences*, 5, (2002).

[Zhan93] Zhang M. On nontotients, *J. Number Theory*, 43(2), 168–172, (1993).

This page intentionally left blank

Index

321 number, 284, 390
321 primes, 284
321 primes of the second kind, 285
(α, β)-amicable pairs, 383
(α, β)-multiple amicable pair, 340, 387
$\frac{1}{m}$-sociable number of order k, 353

A

absolute primes, 387
abundance, 179, 336
abundancy, 336
abundancy index, 336
abundant number, 121, 179, 383
additive function, 36
aliquot k-cycle, 345, 390
aliquot part, 2, 345
aliquot sequence, 346
aliquot sum, 95, 119, 239, 345
aliquot sum function, 95, 119, 239, 345
almost k-superperfect numbers, 383
almost m-superperfect numbers, 324
almost perfect number, 320, 383
almost superperfect number, 323, 383
amicable k-cycle, 345
amicable k-tuple, 334, 384
amicable 4-cycle, 121
amicable multisets, 334, 384
amicable numbers, 383
amicable pair, 238, 383
amicable quadruple, 335
amicable triples, 334, 384
anti-prime number, 191, 383, 386
arithmetic function, 35
aspiring number, 283, 350
augmented amicable numbers, 342

B

betrothed numbers, 342, 384, 388
bi-unitary divisor, 99, 330
bi-unitary multiperfect numbers, 384
bi-unitary multiply k-perfect numbers, 384
bi-unitary multiply perfect number, 330
bi-unitary perfect number, 330, 384
binomial coefficients, 384
biquadratic number, 212, 384
block factor, 328
Borho and Hoffmann's rule, 251
Borho's rule, 360
Boro rule, 255

C

Carmichael number, 63, 384
Carol number, 203, 384
Catalan's conjecture, 283, 351, 367
Catalan–Dickson conjecture, 367
ceiling function, 42
centered m-gonal numbers, 384
centered enneagonal number, 147, 211
centered nonagonal number, 147, 211
Chebyshev function, 79
Chen primes, 384
colossally abundant number, 189, 384
completely additive function, 37
completely multiplicative function, 37
composite number, 59
constructible numbers, 384
continued fraction, 26
cototient number, 55, 385
cube numbers, 385
cubic numbers, 385
Cullen numbers, 385
Cullen numbers of the second kind, 391
cycle sums, 348

D

defective number, 177
deficiency, 177
deficient number, 120, 177, 385
Dirichlet L-function, 81
Dirichlet character, 81
Dirichlet's theorem on primes in arithmetic progressions, 82
division algorithm, 1
divisor, 2
divisor function, 86
double Mersenne number, 201, 385
double Mersenne prime, 202
double perfect number, 202

E

Eisenstein amicable numbers, 288
Eisenstein integers, 206
Eisenstein Mersenne numbers, 385
Eisenstein Mersenne primes, 206
Eisenstein perfect numbers, 206
emirps, 385
Erdős–Nicolas numbers, 312, 385
Euclid–Euler theorem, 123
Euclidean algorithm, 5
Euler's rule, 245
Euler's theorem, 245
Euler's totient function, 50
even amicable pair, 260
even–odd amicable pair, 261
evil numbers, 215, 385
excessive number, 179, 383

F

Fermat number, 69, 206, 385
Fermat pseudoprimes, 385
Fibonacci numbers, 385
floor function, 42
Friedman numbers, 385
friendly k-tuple, 336, 385
friendly club, 385
friendly number, 336, 385
friendly pair, 336, 385

G

g-Niven numbers, 386
g-harshad numbers, 386
Gaussian amicable pair, 287
Gaussian amicable numbers, 287
Gaussian integers, 205, 287
Gaussian Mersenne numbers, 385
Gaussian Mersenne prime, 205
Gaussian perfect numbers, 205
Gaussian prime, 205
generalized k-super abundant number, 188, 385
generalized aliquot sequence, 352
gigantic primes, 386
Goldbach numbers, 386
Granville numbers, 325, 386, 389

H

harmonic divisor number, 200, 386–387
harmonic mean, 200
harshad numbers, 386
hemiperfect numbers, 386
hexagonal number, 210
highly abundant number, 184, 386
highly composite number, 191, 383, 385–386
highly cototient numbers, 386
hyperperfect number, 317, 386

I

irreducible pseudoperfect number, 307, 389
irreducible semiperfect number, 307, 389

J

Jacobi symbol, 20

K

k-dimensional hypercube numbers, 386
k-fold perfect, 313
k-fold perfect numbers, 387
k-friable numbers, 389
k-hemiperfect numbers, 386
k-hyperperfect number, 317, 386
k-perfect, 313
k-perfect numbers, 387
k-smooth numbers, 389
k-superperfect numbers, 390
k-tuple of sociable numbers, 345
Kynéa number, 203, 386

L

least deficient number, 320, 383
Lee's rule, 254
Legendre symbol, 19
Lehmer five, 367
Lucas numbers, 387

M

m-gonal numbers, 387
m-gonal pyramidal numbers, 387
m-superperfect numbers, 324
(m, k)-perfect numbers, 324, 387
Möbius function, 46
megaprimes, 387
Mersenne number, 70, 123, 201, 387
Mersenne primes, 123
monodigits, 389
multi-amicable pairs, 383, 387
multiperfect number, 313
multiple, 2
multiple amicable pairs, 383
multiple perfect number, 313
multiplicative function, 36
multiplicative order, 22
multiply perfect number, 313, 387

N

Niven numbers, 386
non-cototient number, 56, 387
non-totient number, 54, 387
number of divisors' function, 87, 89
number-theoretic function, 35
numeral palindromes, 387
numeric palindromes, 387

O

odd amicable pairs, 261
odd perfect number, 127
odious numbers, 215, 387
order of the set of sociable numbers, 346
Ore harmonic number, 153, 200, 386
Ore number, 200, 386, 387

P

palindromic numbers, 387
panarithmic number, 195, 388
Pascal's triangle, 212, 384
perfect number, 107, 388
perfect totient number, 331, 388
period of the social sequence, 346
permutable primes, 205, 387

pernicious number, 214, 388
Pierpont numbers, 286
Pierpont primes, 286, 388
Pierpont primes of the second kind, 388
pluperfect number, 313
polite number, 207, 388
Poulet number, 62, 388
practical number, 195, 388
primary pseudoperfect number, 307
prime counting function, 72
prime number, 59
prime number theorem, 75
primitive abundant number, 182, 383
primitive friendly pair, 339
primitive pseudoperfect number, 307, 389
primitive semiperfect number, 307
primitive weird number, 309, 391
primorial, 388
pronic numbers, 388
proper divisor, 345
Proth numbers, 388
pseudoperfect number, 305, 389

Q

quasi k-superperfect numbers, 388
quasi m-superperfect numbers, 324
quasi-aliquot sequence, 352
quasi-amicable numbers, 342, 384, 388
quasi-perfect numbers, 388
quasi-sociable k-tuples, 388
quasi-sociable chain, 352, 388
quasi-sociable number of order k, 352
quasi-sociable numbers, 351, 388
quasi-sociable sequence, 352, 388
quasi-superperfect number, 323, 388

R

Ramanujan–Nagell numbers, 144, 389
reduced aliquot sequence, 352
reduced amicable numbers, 342, 384, 388
reduced sociable numbers, 351
refactorable number, 316, 389
relatively prime amicable pairs, 263
repdigits, 389
repunits, 389
restricted divisor function, 95, 119, 239, 345
Riesel numbers, 389
Robin's inequality, 188

S

$\mathcal{S}$-abundant numbers, 386
$\mathcal{S}$-deficient numbers, 386
$\mathcal{S}$-perfect numbers, 325, 386, 389
safe prime, 160, 389
Sarrus numbers, 388
semiperfect number, 305, 389
semiprimes, 389
Sierpiński numbers, 389
sigma function, 87, 93, 345
slightly abundant numbers, 388
slightly defective number, 320, 383
sociable k-cycle, 345
sociable k-tuples, 390
sociable 4-cycle, 121
sociable chain, 349
sociable groups of order k, 390
sociable numbers, 345, 390
sociable of order k, 349
sociable quadruple, 121
sociable sequence, 349
solitary number, 336, 338, 390
Sophie Germain prime, 160, 390
square number, 211
square-free integers, 390
square-free numbers, 390
strobogrammatic numbers, 390
sublime numbers, 390
sum of divisors' function, 87, 93, 120, 345
sum of the xth powers of the divisors' function, 86

sum of the xth powers of the unitary divisors function, 97
superabundant number, 185, 385
superior highly composite number, 193, 390
superperfect number, 322, 390

T

tau function, 87, 89
tau number, 316, 389
te Riele's algorithm, 278
Thābit ibn Qurra number, 284, 390
Thābit ibn Qurra theorem, 242
Thābit numbers, 244, 284, 390
Thābit numbers of the second kind base b, 285, 390
Thābit numbers base b, 285, 390
Thābit numbers of the second kind, 390
Thābit prime base b, 286, 390
Thābit primes, 245, 284, 390
Thābit primes of the second kind, 285, 390
Thābit primes of the second kind base b, 390
Thābit's rule, 242
titanic primes, 391
totient number, 53, 391
trapecoidal numbers, 207, 391
triangular number, 210, 391
twin amicable pair, 266

U

unitary k-perfect number, 330
unitary divisor, 97, 328
unitary divisor function, 97
unitary multiply perfect number, 330
unitary perfect number, 328, 391
untouchable number, 310, 391

V

von Mangoldt function, 79

W

Wagstaff primes, 391
weird number, 308, 391
Wiethaus's rule, 257
Williams number of the second kind base b, 285, 391
Williams numbers base b, 285, 391
Williams prime base b, 286, 391
Williams primes of the second kind base b, 391
Woodall number, 202, 391